

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-146963
Filing date: 17 May 2004 (17.05.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 5 月 1 7 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 1 4 6 9 6 3

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
J P 2 0 0 4 - 1 4 6 9 6 3
The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 1 3 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048160197
【提出日】 平成16年 5月17日
【あて先】 特許庁長官 殿
【国際特許分類】 G09L 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 野仲 真佐男
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 布田 裕一
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 横田 薫
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 宮▲ざき▼ 雅也
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 山本 雅哉
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 村瀬 薫
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【先の出願に基づく優先権主張】
 【出願番号】 特願2004-110069
 【出願日】 平成16年 4月 2日
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】 特許請求の範囲

【請求項 1】

不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
前記コンテンツを、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、実行装置へ配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を取得する取得部と、
認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、
前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。

【請求項 2】

前記コンテンツは、前記実行装置で実行可能なプログラムであり、
前記実行部は、前記プログラムを実行すること、
を特徴とする請求項 1 に記載の不正コンテンツ検知システム。

【請求項 3】

コンテンツを実行、もしくは再生する実行装置であって、
前記実行装置は、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、
認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、
前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする実行装置。

【請求項 4】

前記取得部は、可搬媒体からデータを取得すること、
を特徴とする、請求項 3 に記載の実行装置。

【請求項 5】

前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取

得すること、

を特徴とする、請求項 3 に記載の実行装置。

【請求項 6】

前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、

を特徴とする、請求項 3 から請求項 5 のいずれか 1 項に記載の実行装置。

【請求項 7】

前記実行装置は、さらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、

前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、

前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、

を特徴とする、請求項 3 から請求項 6 のいずれか 1 項に記載の実行装置。

【請求項 8】

前記実行装置は、さらに、

前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、

前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、

を特徴とする、請求項 7 に記載の実行装置。

【請求項 9】

前記実行装置は、さらに、

デバイス鍵を保持するデバイス鍵格納部と、

前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、

前記取得部はさらに、前記暗号化鍵束を受信すること、

を特徴とする、請求項 7 または請求項 8 に記載の実行装置。

【請求項 10】

前記取得部は、 m 個 (m は 2 以上の自然数) の前記コンテンツ位置情報と、前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する m 個の前記認証情報の中から、 b 組 (b は 1 以上 $m-1$ 以下の自然数) の前記コンテンツ位置情報及び前記認証情報を取得し、

前記検証部は、前記コンテンツ及び m 個の前記コンテンツ位置情報を基に、 m 個の前記代表部分コンテンツを取得し、 m 個の前記代表部分コンテンツ及び m 個の前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、

を特徴とする、請求項 3 から請求項 9 のいずれか 1 項に記載の実行装置。

【請求項 11】

前記取得部は、 m 組の前記コンテンツ位置情報及び前記認証情報の中から、 b 組の前記コンテンツ位置情報及び前記認証情報をランダムに選択すること、

を特徴とする、請求項 10 に記載の実行装置。

【請求項 12】

前記取得部は、 m 組の前記コンテンツ位置情報及び前記認証情報の中から、 b 組の前記コンテンツ位置情報及び前記認証情報を順番に選択すること、

を特徴とする、請求項 10 に記載の実行装置。

【請求項 13】

前記取得部において、 b は 1 であること、

を特徴とする、請求項 10 から請求項 12 のいずれか 1 項に記載の実行装置。

【請求項 14】

前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、

を特徴とする、請求項 3 から請求項 13 のいずれか 1 項に記載の実行装置。

【請求項 15】

前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、

を特徴とする、請求項 3 から請求項 13 のいずれか 1 項に記載の実行装置。

【請求項 16】

前記検証情報は、デジタル署名方式の検証鍵であること、

を特徴とする、請求項 3 から請求項 13 のいずれか 1 項に記載の実行装置。

【請求項 17】

前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、

前記取得部はさらに、前記検証情報識別子を受信し、

前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、

を特徴とする、請求項 3 から請求項 16 のいずれか 1 項に記載の実行装置。

【請求項 18】

前記取得部はさらに、前記検証情報を受信すること、

を特徴とする、請求項 3 から請求項 17 のいずれか 1 項に記載の実行装置。

【請求項 19】

前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、

前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、

を特徴とする、請求項 16 から請求項 18 のいずれか 1 項に記載の実行装置。

【請求項 20】

前記実行装置は、さらに、

前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、

を特徴とする、請求項 19 に記載の実行装置。

【請求項 21】

前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、

を特徴とする、請求項 20 に記載の実行装置。

【請求項 22】

前記第二取得部と前記取得部は等しいこと、

を特徴とする、請求項 20 または請求項 21 に記載の実行装置。

【請求項 23】

前記コンテンツは、前記実行装置で実行可能なプログラムであり、

前記実行部は、前記プログラムを実行すること、

を特徴とする請求項 3 から請求項 22 のいずれか 1 項に記載の実行装置。

【請求項 24】

コンテンツを配布する配布センタであって、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、

前記コンテンツと、前記認証情報と、を配布する配布部と、
を備えることを特徴とする配布センタ。

【請求項 25】

前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、

を特徴とする、請求項 24 に記載の配布センタ。

【請求項 26】

前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、

を特徴とする、請求項 24 または請求項 25 に記載の配布センタ。

【請求項 27】

前記配布センタはさらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、

前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、

前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、

を特徴とする、請求項 24 から請求項 26 のいずれか 1 項に記載の配布センタ。

【請求項 28】

前記配布センタはさらに

一以上のデバイス鍵を保持する実行装置情報格納部と、

前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、

前記配布部はさらに、前記暗号化鍵束を配布すること、

を特徴とする、請求項 27 に記載の配布センタ。

【請求項 29】

前記配布センタはさらに

前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、

前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、

を特徴とする、請求項 27 または請求項 28 に記載の配布センタ。

【請求項 30】

前記コンテンツ位置情報格納部は、 m 個（ m は 2 以上の自然数）の前記コンテンツ位置情報及び前記コンテンツを保持し、

前記認証情報生成部は、 m 個の前記コンテンツ位置情報及び前記コンテンツを基に、 m 個の前記代表部分コンテンツを取得し、 m 個の前記代表部分コンテンツ及び前記認証情報生成情報を基に、 m 個の認証情報を生成し、

前記取得部は、前記コンテンツ位置情報と前記認証情報の m 組を配布すること、

を特徴とする、請求項 24 から請求項 29 のいずれか 1 項に記載の配布センタ。

【請求項 31】

前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、

を特徴とする、請求項 24 から請求項 30 のいずれか 1 項に記載の配布センタ。

【請求項 32】

前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、

を特徴とする、請求項 24 から請求項 30 のいずれか 1 項に記載の配布センタ。

【請求項 33】

前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項 24 から請求項 32 のいずれか 1 項に記載の配布センタ。

【請求項 34】

前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、

を特徴とする、請求項 24 から請求項 33 のいずれか 1 項に記載の配布センタ。

【請求項 35】

前記配布センタはさらに、

前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、

を特徴とする、請求項 24 から請求項 34 のいずれか 1 項に記載の配布センタ。

【請求項 36】

前記コンテンツ位置情報生成部はさらに、

外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、

を特徴とする、請求項 35 に記載の配布センタ。

【請求項 37】

前記コンテンツ位置情報生成部はさらに、

ランダムに前記コンテンツ位置情報を生成すること、

を特徴とする、請求項 35 に記載の配布センタ。

【請求項 38】

コンテンツを実行、もしくは再生するコンテンツ実行方法であって、

前記コンテンツ実行方法は、

前記コンテンツの一部である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、

前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、

認証情報を検証するための検証情報を保持するステップと、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、

前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、

を含むことを特徴とするコンテンツ実行方法。

【請求項 39】

コンテンツを実行、もしくは再生するコンテンツ実行プログラムであって、

前記コンテンツ実行プログラムは、

前記コンテンツの一部である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、

前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、

認証情報を検証するための検証情報を保持するステップと、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、

前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、

を含むことを特徴とする実行プログラム。

【請求項 40】

請求項 39 に記載のプログラムを記録した媒体。

【請求項 41】

コンテンツを実行、もしくは再生するコンテンツ実行装置の集積回路であって、
前記集積回路は、

前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、

認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、

前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする集積回路。

【請求項 4 2】

コンテンツを配布するコンテンツ配布方法であって、

前記コンテンツ配布方法は、

認証情報生成情報を保持するステップと、

前記コンテンツを入力するステップと、

前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、

前記コンテンツと、前記認証情報と、を配布するステップと、

を含むことを特徴とするコンテンツ配布方法。

【請求項 4 3】

コンテンツを配布する処理をコンピュータに実行させるプログラムであって、

前記コンテンツ配布プログラムは、

前記コンテンツを入力するステップと、

認証情報生成情報を保持するステップと、

前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、

前記コンテンツと、前記認証情報と、を配布するステップと、

を含むことを特徴とするコンピュータプログラム。

【請求項 4 4】

請求項 4 3 に記載のプログラムを記録した媒体。

【請求項 4 5】

コンテンツを配布する配布センタにおける集積回路であって、

前記集積回路は、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、

前記コンテンツと、前記認証情報と、を配布する配布部と、

を備えることを特徴とする集積回路。

【請求項 46】

不正コンテンツを検知する不正コンテンツ検知システムであって、

前記不正コンテンツ検知システムは、

可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ取得し、それぞれの前記第一属性値を含むヘッダ情報を生成するヘッダ情報生成部と、

前記ヘッダ情報及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、

前記コンテンツと、前記ヘッダ情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、

前記実行装置は、

前記コンテンツと、前記ヘッダ情報と、前記認証情報と、を取得する取得部と、

前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記検証情報を基に、前記認証情報が前記ヘッダ情報の認証情報であるかどうか検証する認証情報検証部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、

前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第二属性値を取得し、それぞれの前記第二属性値と、前記ヘッダ情報に含まれる前記第二属性値の前記特定情報に対応するそれぞれの前記第一属性値を比較するヘッダ情報検証部と、

前記認証情報検証部及び前記ヘッダ情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする不正コンテンツ検知システム。

【書類名】 明細書

【発明の名称】 不正コンテンツ検知システム

【技術分野】

【0001】

本発明は不正なコンテンツを検知する技術に関するものである。

【背景技術】

【0002】

近年、デジタルコンテンツの普及に伴い、著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる違法コンテンツの不正配布が社会問題となってきた。このコンテンツ不正配布の一つのケースとして、映画館等で上映される映画コンテンツを著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した動画コンテンツを光ディスクに記録し販売するというものが挙げられる。

【0003】

上記のようなコンテンツ不正利用を防ぐ方法の従来技術としては、特許文献1に記載されている不正コンテンツ検知システムが知られている。この従来技術は、可搬媒体の中に、コンテンツデータの他に、複数の部分コンテンツデータに対応するハッシュ値と、複数の部分コンテンツデータを結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前と、コンテンツを再生している途中に、記録されたコンテンツデータが正規の著作権者によって記録されたものか、デジタル署名及びハッシュ値を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを正しく再生しない。これにより、不正なコンテンツの配布防止につながる。

【0004】

ここでは、従来技術の詳細の一例を図52を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。

初めに、正規の著作権者が、コンテンツデータと、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツを c 個（ c は2以上の自然数）のコンテンツブロック（図32のコンテンツブロック $BLK1 \cdots BLKc$ に対応）に分割する。そして、一方向性関数を用いてコンテンツブロック $BLK1$ のハッシュ値 $HASH1$ を計算する。コンテンツブロック $BLK2$ 以降も同様にハッシュ値を計算し、それぞれのコンテンツブロック $BLK2$ 、 \cdots 、 $BLKc$ に対応するハッシュ値 $HASH2$ 、 \cdots 、 $HASHc$ を求める。そして、 c 個のハッシュ値 $HASH1$ 、 \cdots 、 $HASHc$ を連結させたものをヘッダ情報 $HEAD$ とする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報 $HEAD$ のデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。

【0005】

続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始する。その後、実行装置はコンテンツを再生しながら、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテンツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。

【0006】

このような従来技術により、何らかの理由によりコンテンツが盗み出され、そのコンテ

ンツを可搬媒体に記録して販売しようとしても、可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正なコンテンツ流通に対する対策が可能となる。

【特許文献1】 米国特許第6480961号明細書

【特許文献2】 特開2002-281013号公報

【非特許文献1】 「情報セキュリティ」宮地充子・菊池浩明編著 情報処理学会編集

【非特許文献2】 「THE ART OF COMPUTER PROGRAMMING Vol. 2 ~ SEMINUMERICAL ALGORITHMS」 DONALD E. KNUTH 著、ISBN 0-201-03822-6

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、前記従来技術では、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという課題を有していた。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【0008】

本発明は、前記従来技術の課題を解決するもので、コンテンツ再生中の実行装置の処理負荷を軽減させた不正コンテンツ検知システムを提供することを目的とする。

【課題を解決するための手段】

【0009】

請求項1における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、前記コンテンツを、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、実行装置へ配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を取得する取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0010】

請求項2における発明は、請求項1に記載の不正コンテンツ検知システムであって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

請求項3における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得す

る取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0011】

請求項4における発明は、請求項3に記載の実行装置であって、前記取得部は、可搬媒体からデータを取得すること、を特徴とする。

請求項5における発明は、請求項3に記載の実行装置であって、前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、を特徴とする。

【0012】

請求項6における発明は、請求項3から請求項5のいずれか1項に記載の実行装置であって、前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、を特徴とする。

請求項7における発明は、請求項3から請求項6のいずれか1項に記載の実行装置であって、前記実行装置は、さらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、を特徴とする。

【0013】

請求項8における発明は、請求項7に記載の実行装置であって、前記実行装置は、さらに、前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、を特徴とする。

請求項9における発明は、請求項7または請求項8のいずれかに記載の実行装置であって、前記実行装置は、さらに、デバイス鍵を保持するデバイス鍵格納部と、前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、前記取得部はさらに、前記暗号化鍵束を受信すること、を特徴とする。

【0014】

請求項10における発明は、請求項3から請求項9のいずれか1項に記載の実行装置であって、前記取得部は、 m 個（ m は2以上の自然数）の前記コンテンツ位置情報と、前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する m 個の前記認証情報の中から、 b 組（ b は1以上 $m-1$ 以下の自然数）の前記コンテンツ位置情報及び前記認証情報を取得し、前記検証部は、前記コンテンツ及び m 個の前記コンテンツ位置情報を基に、 m 個の前記代表部分コンテンツを取得し、 m 個の前記代表部分コンテンツ及び m 個の前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【0015】

請求項11における発明は、請求項10に記載の実行装置であって、前記取得部は、 m 組の前記コンテンツ位置情報及び前記認証情報の中から、 b 組の前記コンテンツ位置情報及び前記認証情報をランダムに選択すること、を特徴とする。

請求項12における発明は、請求項10に記載の実行装置であって、前記取得部は、 m 組の前記コンテンツ位置情報及び前記認証情報の中から、 b 組の前記コンテンツ位置情報及び前記認証情報を順番に選択すること、を特徴とする。

【0016】

請求項13における発明は、請求項10から請求項12のいずれか1項に記載の実行装置であって、前記取得部において、 b は1であること、を特徴とする。

請求項14における発明は、請求項3から請求項13のいずれか1項に記載の実行装置

であって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

【００１７】

請求項１５における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。

請求項１６における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記検証情報は、デジタル署名方式の検証鍵であること、を特徴とする。

【００１８】

請求項１７における発明は、請求項３から請求項１６のいずれか１項に記載の実行装置であって、前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、前記取得部はさらに、前記検証情報識別子を受信し、前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【００１９】

請求項１８における発明は、請求項３から請求項１７のいずれか１項に記載の実行装置であって、前記取得部はさらに、前記検証情報を受信すること、を特徴とする。

請求項１９における発明は、請求項１６から請求項１８のいずれか１項に記載の実行装置であって、前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【００２０】

請求項２０における発明は、請求項１９に記載の実行装置であって、前記実行装置は、さらに、前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、を特徴とする。

請求項２１における発明は、請求項２０に記載の実行装置であって、前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、を特徴とする。

【００２１】

請求項２２における発明は、請求項２０または請求項２１に記載の実行装置であって、前記第二取得部と前記取得部は等しいこと、を特徴とする。

請求項２３における発明は、請求項３から請求項２２のいずれか１項に記載の実行装置であって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

【００２２】

請求項２４における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を配布する配布部と、を備えることを特徴とする。

【００２３】

請求項２５における発明は、請求項２４に記載の配布センタであって、前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、を特徴とする。

請求項 26 における発明は、請求項 24 または請求項 25 に記載の配布センタであって、前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、を特徴とする。

【0024】

請求項 27 における発明は、請求項 24 から請求項 26 のいずれか 1 項に記載の配布センタであって、前記配布センタはさらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、を特徴とする。

【0025】

請求項 28 における発明は、請求項 27 に記載の配布センタであって、前記配布センタはさらに、一以上のデバイス鍵を保持する実行装置情報格納部と、前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、前記配布部はさらに、前記暗号化鍵束を配布すること、を特徴とする。

【0026】

請求項 29 における発明は、請求項 27 または請求項 28 に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、を特徴とする。

請求項 30 における発明は、請求項 24 から請求項 29 のいずれか 1 項に記載の配布センタであって、前記コンテンツ位置情報格納部は、 m 個 (m は 2 以上の自然数) の前記コンテンツ位置情報及び前記コンテンツを保持し、前記認証情報生成部は、 m 個の前記コンテンツ位置情報及び前記コンテンツを基に、 m 個の前記代表部分コンテンツを取得し、 m 個の前記代表部分コンテンツ及び前記認証情報生成情報を基に、 m 個の認証情報を生成し、前記取得部は、前記コンテンツ位置情報と前記認証情報の m 組を配布すること、を特徴とする。

【0027】

請求項 31 における発明は、請求項 24 から請求項 30 のいずれか 1 項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

請求項 32 における発明は、請求項 24 から請求項 30 のいずれか 1 項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。

【0028】

請求項 33 における発明は、請求項 24 から請求項 32 のいずれか 1 項に記載の配布センタであって、前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、を特徴とする。

請求項 34 における発明は、請求項 24 から請求項 33 のいずれか 1 項に記載の配布センタであって、前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、を特徴とする。

【0029】

請求項 35 における発明は、請求項 24 から請求項 34 のいずれか 1 項に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、を特徴とする。

請求項 36 における発明は、請求項 35 に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに、外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、を特徴とする。

【0030】

請求項 37 における発明は、請求項 35 に記載の配布センタであって、前記コンテンツ

位置情報生成部はさらに、ランダムに前記コンテンツ位置情報を生成すること、を特徴とする。

請求項 38 における発明は、コンテンツを実行、もしくは再生するコンテンツ実行方法であって、前記コンテンツ実行方法は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、認証情報を検証するための検証情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、を含むことを特徴とする。

【0031】

請求項 39 における発明は、コンテンツを実行、もしくは再生するコンテンツ実行プログラムであって、前記コンテンツ実行プログラムは、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、認証情報を検証するための検証情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、を含むことを特徴とする。

【0032】

請求項 40 における発明は、請求項 39 に記載のプログラムを記録した媒体であることを特徴とする。

請求項 41 における発明は、コンテンツを実行、もしくは再生するコンテンツ実行装置の集積回路であって、前記集積回路は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0033】

請求項 42 における発明は、コンテンツを配布するコンテンツ配布方法であって、前記コンテンツ配布方法は、認証情報生成情報を保持するステップと、前記コンテンツを入力するステップと、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、前記コンテンツと、前記認証情報と、を配布するステップと、を含むことを特徴とする。

【0034】

請求項 43 における発明は、コンテンツを配布する処理をコンピュータに実行させるプログラムであって、前記コンテンツ配布プログラムは、前記コンテンツを入力するステップと、認証情報生成情報を保持するステップと、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテ

ツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、前記コンテンツと、前記認証情報と、を配布するステップと、を含むことを特徴とする。

【0035】

請求項44における発明は、請求項43に記載のプログラムを記録した媒体であることを特徴とする。

請求項45における発明は、コンテンツを配布する配布センタにおける集積回路であって、前記集積回路は、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を配布する配布部と、を備えることを特徴とする。

【0036】

請求項46における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ取得し、それぞれの前記第一属性値を含むヘッダ情報を生成するヘッダ情報生成部と、前記ヘッダ情報及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記ヘッダ情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記ヘッダ情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記検証情報を基に、前記認証情報が前記ヘッダ情報の認証情報であるかどうかを検証する認証情報検証部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第二属性値を取得し、それぞれの前記第二属性値と、前記ヘッダ情報に含まれる前記第二属性値の前記特定情報に対応するそれぞれの前記第一属性値を比較するヘッダ情報検証部と、前記認証情報検証部及び前記ヘッダ情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【発明の効果】

【0037】

本発明の不正コンテンツ検知システムによれば、コンテンツを実行開始、もしくは再生開始する前にのみ、コンテンツが正規の著作権者により配布されたコンテンツ（正規コンテンツ）なのか、正規の著作権者以外により配布されたコンテンツ（不正コンテンツ）なのかを検証し、コンテンツの実行中、再生中にはその検証を行わないようにした。そうすることにより、不正コンテンツの実行、再生を制限（開始不許可など）することが出来るようになるとともに、従来技術に比べ、コンテンツ実行中、再生中の実行装置の処理負荷を軽減出来るようになった。

【0038】

また、実施の形態1及び2における不正コンテンツ検知システムでは、実行装置がコン

テンツを実行、再生開始する場合に、コンテンツに付随するコンテンツ位置情報に対応するコンテンツの一部分である、部分コンテンツの属性値（ハッシュ値）を検証のするようにした。この際、コンテンツ位置情報を暗号化しておくことによって、不正者は、コンテンツのどの一部分が検証されるのか予測出来ないようになった。この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証するようにコンテンツ位置情報に記載されている場合、で実行、再生の制限（再生不許可など）が出来るようになった。なお、コンテンツ位置情報には、例えば、その部分のデータを変えてしまうとコンテンツ全体に影響を与えるようなコンテンツの特徴点（例えば、MP E GデータにおけるIピクチャなど）を選択すると効果的となる。

【0039】

実施の形態3における不正コンテンツ検知システムでは、実行装置が同じコンテンツを実行、再生する場合にも、コンテンツの中の毎回異なる一部分の部分コンテンツの属性値（ハッシュ値）を検証するようにした。これにより、不正者は、次にコンテンツのどの一部分が検証されるのか予測出来ないようになった。この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、ある確率（実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証する場合）で実行、再生の制限（再生不許可など）が出来るようになった。

【0040】

このことにより、コンテンツの中の一部を、不正なコンテンツに差し替えられるような攻撃を防ぐ抑止力となる。これは、コンテンツデータとともに、そのコンテンツデータ全体に対する属性値（ハッシュ値）1つと、その属性値（ハッシュ値）に対するデジタル署名と、を記録した可搬媒体を配布する自明な方式に比べても優位性を持つ。何故なら、自明な方式の場合コンテンツデータ全体に対する属性値（ハッシュ値）を計算しなくてはならないため、コンテンツの実行、再生開始前の処理に時間がかかっていた。しかし、本発明の不正コンテンツ検知システムによれば、コンテンツの実行、再生開始前には、コンテンツデータの中の一部、もしくは毎回異なる一部分の部分コンテンツの属性値（ハッシュ値）だけを計算すれば良いので、自明な方式に比べ、処理時間を短縮することが出来る。

【発明を実施するための最良の形態】

【0041】

以下本発明の実施の形態について、図面を参照しながら説明する。

（実施の形態1）

図1は、本発明の実施の形態1における不正コンテンツ検知システムの構成図である。図1において、配布センタ10は外部からコンテンツCNTを受け取り、後述する実行装置12がコンテンツCNTを実行するために必要となる情報を後述する可搬媒体11に記録するものであり、可搬媒体11は実行装置12がコンテンツCNTを実行するために必要となる情報が記録されているものであり、複数の実行装置12は可搬媒体11に記録されている情報を用いて、コンテンツCNTを実行するものである。

【0042】

不正コンテンツ検知システム1は、配布センタ10（正規のコンテンツ提供者、著作権者）が、DVD-ROM等の可搬媒体11の配布手段によって、暗号化されたコンテンツCNTである暗号化コンテンツENCNTと、コンテンツCNTを基に生成されるヘッダ情報HEADのデジタル署名である認証情報AUTHを、各実行装置12へ配布する。各実行装置12は、暗号化コンテンツENCNTを復号化してコンテンツCNTを取得し、認証情報AUTHが配布センタ10によるヘッダ情報HEADの正規のデジタル署名であることと、ヘッダ情報HEADがコンテンツCNTを基に生成されたものであることを確認し、コンテンツCNTを実行開始する。

【0043】

以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一

実施形態である不正コンテンツ検知システム 1 の詳細について説明を行う。

＜不正コンテンツ検知システム 1 の構成＞

不正コンテンツ検知システム 1 は、図 1 に示すように、配布センタ 1 0 と、可搬媒体 1 1 と、 n 個の実行装置 1 2 (n は 1 以上の自然数) から構成される。

【0044】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ 1 0 の構成と動作について述べ、続いて可搬媒体 1 1 の構成について述べ、最後に実行装置 1 2 の構成と動作について述べる。

＜配布センタ 1 0 の構成＞

配布センタ 1 0 は、図 2 に示すように、入力部 1 0 0 1、コンテンツ鍵生成部 1 0 0 2、実行装置情報格納部 1 0 0 3、暗号化鍵束生成部 1 0 0 4、コンテンツ位置情報生成部 1 0 0 5、ヘッダ情報生成部 1 0 0 6、認証情報生成情報格納部 1 0 0 7、認証情報生成部 1 0 0 8、暗号化部 1 0 0 9、配布部 1 0 1 0 から構成される。

【0045】

(1) 入力部 1 0 0 1

入力部 1 0 0 1 は、外部からコンテンツ C N T を入力出来るものである。入力部 1 0 0 1 は、例えば、可搬媒体である D V D - R O M 等からコンテンツ C N T を読み取る機能を有する。外部から入力されるコンテンツ C N T は、例えば図 3 で示すように、 c 個の部分コンテンツ C N T - 1、 \dots 、C N T - c から構成されているとする。また、それぞれの部分コンテンツは、特定情報によって特定可能であるとする。この特定情報は、例えば、部分コンテンツの先頭を表す物理アドレスやセクタ情報、サイズ、コンテンツの先頭からの経過時間などであるが、部分コンテンツを特定可能な情報であれば、どのような情報でも良く、さらには、上記情報を組み合わせた情報であっても良い。さらに、コンテンツ C N T (部分コンテンツ C N T - 1、 \dots 、C N T - c) は、実行装置 1 2 で実行可能なフォーマット形式であって、例えば、M P E G フォーマットによる動画データや M P 3 フォーマットによる音声データなどである。外部からコンテンツ C N T が入力された場合、そのコンテンツ C N T をコンテンツ鍵生成部 1 0 0 2 へ出力する。例えば、 c は 1 0 0 0 0 0 であるが、 c は 1 以上の自然数であればどのような値でも良い。

【0046】

(2) コンテンツ鍵生成部 1 0 0 2

コンテンツ鍵生成部 1 0 0 2 は、入力部 1 0 0 1 からコンテンツ C N T が入力された場合、コンテンツ鍵 C K を生成する。コンテンツ鍵 C K を生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。乱数を生成する方法については、非特許文献 2 が詳しい。そして、コンテンツ鍵 C K 及びコンテンツ C N T を暗号化鍵束生成部 1 0 0 4 へ出力する。なお、コンテンツ鍵 C K はコンテンツ C N T、及び、コンテンツ位置情報 P O S を暗号化、復号化するための鍵であり、暗号化部 1 0 0 9 及び実行装置 1 2 のコンテンツ位置情報取得部 1 2 4 及び部分復号化部 1 2 7 で使用される。

【0047】

(3) 実行装置情報格納部 1 0 0 3

実行装置情報格納部 1 0 0 3 は、複数の実行装置 1 2 に与えられる鍵情報を保持するものである。図 4 は、実行装置情報格納部 1 0 0 3 の一例を示しており、装置識別子 A I D 1 に対応付けられたデバイス鍵 D K 1 と、装置識別子 A I D 2 に対応付けられたデバイス鍵 D K 2 と、 \dots 、装置識別子 A I D n に対応付けられたデバイス鍵 D K n を保持している状態を示している。ここで、装置識別子 A I D 1、 \dots 、A I D n のそれぞれは、複数の実行装置 1 2 のいずれかに対応付けられており、デバイス鍵 D K 1、 \dots 、D K n のそれぞれは、対応する実行装置 1 2 のデバイス鍵格納部 1 2 2 に格納されている鍵である。なお、デバイス鍵 D K 1、 \dots 、D K n はコンテンツ鍵 C K を暗号化、復号化するための鍵であり、暗号化鍵束生成部 1 0 0 4 及びコンテンツ鍵取得部 1 2 3 で用いられる。

【0048】

(4) 暗号化鍵束生成部1004

暗号化鍵束生成部1004は、コンテンツ鍵生成部1002からコンテンツ鍵CK及びコンテンツCNTが入力された場合、実行装置情報格納部1003にアクセスして複数の実行装置12が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成するものである。暗号化鍵束KBは、各実行装置12がその暗号化鍵束KBと自身の保持する鍵を用いてコンテンツ鍵CKが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置12はそれぞれ、装置識別子とデバイス鍵の一组をいずれか保持しており、情報格納部1003には、図4のように、実行装置12が保持する装置識別子とデバイス鍵の全ての組が格納されているとする。そのような場合、暗号化鍵束KBは例えば以下のように生成される。実行装置情報格納部1003から装置識別子AID1と対応するデバイス鍵DK1を取得する。そして、デバイス鍵DK1を基にコンテンツ鍵CKを暗号化し、暗号化コンテンツ鍵ENCCK1を生成し、装置識別子AID1に対応付ける。そして、他の装置識別子とデバイス鍵に対しても同様の処理を行い、暗号化コンテンツ鍵ENCCK2、・・・、ENCCKnを生成し、装置識別子AID2、・・・、AIDnに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵をn組含む、図5のような暗号化鍵束KBを生成する。このような暗号化鍵束KBの構成にすることによって、各実行装置12はその暗号化鍵束KBと自身の保持するデバイス鍵を用いてコンテンツ鍵CKが取得出来るようになる。そして、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKをコンテンツ位置情報生成部1005に出力する。なお、特許文献2などに記載の方法を用いることで、暗号化鍵束KBの中の暗号化コンテンツ鍵の数を減らすことや、ある特定の実行装置では正しいコンテンツ鍵を取得出来ないようにして、実行装置を無効化することも出来る。また、暗号化鍵束生成部1004で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES (Advanced Encryption Standard) 方式などであり、実行装置12のコンテンツ鍵取得部123と同じ暗号アルゴリズムを用いる。

【0049】

(5) コンテンツ位置情報生成部1005

コンテンツ位置情報生成部1005は、暗号化鍵束生成部1004から暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力される。そして、まずコンテンツCNTを構成するc個の部分コンテンツCNT—1、・・・、CNT—cの中から、一つの部分コンテンツを選択し、それを代表部分コンテンツP1—CNTとする。ここでは、図6に例として、部分コンテンツCNT—3を代表部分コンテンツP1—CNTとした場合について示している。このc個の部分コンテンツCNT—1、・・・、CNT—cの中から代表部分コンテンツを選択する方法としては、例えば、以下で説明するような3つの方法がある。

【0050】

一つ目の方法は、コンテンツデータのある特徴点（例えば、MPEG動画データにおけるIピクチャやGOPなど）を自動的に選択する方法である。二つ目は、乱数を用いてランダムに自動的に選択する方法である。この二つの方法においては、コンテンツ位置情報生成部1005は、図2で示すような外部から要求情報REQを受け取る機能や外部へコンテンツを出力する機能は必要はない。なお、特徴点（IピクチャやGOPなど）の全てを必ずしも選択する必要はなく、特徴点の一部のみを選択するようにしても良い。そして三つ目は、コンテンツ位置情報生成部1005は外部へコンテンツCNTの中の部分コンテンツを順番に実行する機能を有し、外部から（例えばユーザが）要求信号REQをコンテンツ位置情報生成部1005へ入力したときに実行している部分コンテンツを代表部分コンテンツとするものである。この三つ目の方法は、コンテンツ位置情報生成部1005がディスプレイやキーボードなどの入出力装置を備えることによって実現出来る。

【0051】

そして、その代表部分コンテンツP1—CNTを指し示す特定情報をADDR1とする。そして、続けて、k—1個の代表部分コンテンツP2—CNT、・・・、Pk—CNT

を選択し、その代表部分コンテンツに対応する特定情報をADDR 2、・・・、ADDR kとする（図6参照）。そして、その代表部分コンテンツと特定情報のk組{P 1—CNT、ADDR 1}、{P 2—CNT、ADDR 2}、・・・、{P k—CNT、ADDR k}を、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKと併せて、ヘッダ情報生成部1006へ出力する。kは例えば20であるが、20以外であっても、1以上の自然数であればどのような値でも良く、例えば、代表部分コンテンツと特定情報が一組であってもよい。また、代表部分コンテンツのサイズは、例えば64キロバイトであるが、64キロバイトに限らず、どのようなサイズであっても良く、さらには、代表部分コンテンツ毎に異なるサイズであっても良い。例えば、代表部分コンテンツP 1—CNTが10キロバイトで、代表部分コンテンツP k—CNTが2キロバイトであっても良い。また、選択する部分コンテンツは、コンテンツCNTに応じて変えても良い。

【0052】

（6）ヘッダ情報生成部1006

ヘッダ情報生成部1006は、コンテンツ位置情報生成部1005から、代表部分コンテンツと特定情報のk組{P 1—CNT、ADDR 1}、{P 2—CNT、ADDR 2}、・・・、{P k—CNT、ADDR k}と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、以下のようにして、ヘッダ情報HEADを生成する。まず、代表部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。特定情報識別子を生成する方法としては、自然数を順番に割り当てていく（1、2、・・・、k）方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した特定情報識別子をそれぞれ、ADDR ID 1、ADDR ID 2、・・・ADDR ID kとし、次のように特定情報識別子と代表部分コンテンツと特定情報とが対応しているとする。{ADDR ID 1、P 1—CNT、ADDR 1}、{ADDR ID 2、P 2—CNT、ADDR 2}、・・・、{ADDR ID k、P k—CNT、ADDR k}。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を計算する。代表部分コンテンツのハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献1に記載のSHA-1（Secure Hash Algorithm-1）アルゴリズムやブロック暗号を用いたCBC-MAC（Cipher Block Chaining — Message Authentication Code）などがあり、実行装置12のヘッダ情報検証部128で用いる方法と同じものを用いる。ここで、各組に対して計算したハッシュ値をそれぞれ、HASH 1、HASH 2、・・・HASH kとし、次のように特定情報識別子と代表部分コンテンツと特定情報とハッシュ値が対応しているとする。{ADDR ID 1、P 1—CNT、ADDR 1、HASH 1}、{ADDR ID 2、P 2—CNT、ADDR 2、HASH 2}、・・・、{ADDR ID k、P k—CNT、ADDR k、HASH k}。そして、その中から特定情報識別子と特定情報だけを抽出し、図7で示すような、特定情報識別子と特定情報とを含むコンテンツ位置情報POS={ADDR ID 1、ADDR 1}、{ADDR ID 2、ADDR 2}、・・・、{ADDR ID k、ADDR k}を生成する。また、特定情報識別子とハッシュ値だけを抽出し、図8で示すような、特定情報識別子とハッシュ値とを含むヘッダ情報HEAD={ADDR ID 1、HASH 1}、{ADDR ID 2、HASH 2}、・・・、{ADDR ID k、HASH k}を生成する。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを認証情報生成部1008へ出力する。

【0053】

（7）認証情報生成情報格納部1007

認証情報生成情報格納部1007は、ヘッダ情報HEADの認証情報AUTHを生成するための、認証情報生成情報GENAUTHを保持するものである。この認証情報生成X情報GENAUTHは、例えば、デジタル署名の署名生成鍵である。認証情報生成情報GENAUTHに対応する検証情報VERは、実行装置12の検証情報格納部125に格納されている。この検証情報VERは、例えば、デジタル署名の署名検証鍵である。また、

デジタル署名アルゴリズムは、例えば、非特許文献1に記載のDSA (Digital Signature Algorithm) 方式などである。

【0054】

(8) 認証情報生成部1008

認証情報生成部1008は、ヘッダ情報生成部1006からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKが入力された場合、以下のようにして、ヘッダ情報HEADに対する認証情報AUTHを生成する。まず、認証情報生成情報格納部1007にアクセスして、認証情報生成情報GENAUTHを取得する。そして、ヘッダ情報HEADと認証情報生成情報GENAUTHを用いて、ヘッダ情報HEADの認証情報AUTHを生成する。なお、認証情報AUTHの生成方法の一例は、デジタル署名アルゴリズムであり、k個の特定情報識別子ADDRID1、・・・、ADDRIDkとk個のハッシュ値HASH1、・・・、HASHkを連結した値に対するデジタル署名である。具体的には例えば非特許文献1に記載のDSA方式などであり、実行装置12のヘッダ情報検証部128で用いるデジタル署名検証アルゴリズムと同じデジタル署名アルゴリズムを用いる。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとを暗号化部1009へ出力する。

【0055】

(9) 暗号化部1009

暗号化部1009は、認証情報生成部1008からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとが入力された場合、以下のようにして暗号化コンテンツENCCNTと暗号化コンテンツ位置情報ENCPOSを生成する。まず、コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCCNTを生成する。この暗号化コンテンツENCCNTの生成方法としては、例えば、以下のような方法がある。まず、コンテンツ鍵CKを用いて部分コンテンツCNT-1を暗号化し、暗号化部分コンテンツENCCNT-1を生成する。続いて、同じコンテンツ鍵CKを用いて部分コンテンツCNT-2を暗号化し、暗号化部分コンテンツENCCNT-2を生成する。これを繰り返して、図9で示すような暗号化部分コンテンツENCCNT-1、・・・、ENCCNT-cから構成される暗号化コンテンツを生成する。また、コンテンツ鍵CKを基に、コンテンツ位置情報POSを暗号化し、暗号化コンテンツ位置情報ENCPOSを生成する。そして、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCCNTを配布部1010へ出力する。なお、暗号化部1009で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式などであり、実行装置12のコンテンツ位置情報取得部124及び部分復号化部127と同じ暗号アルゴリズムを用いる。さらに、暗号化コンテンツENCCNTの生成方法として、各部分コンテンツに対して、全て一つの同じコンテンツ鍵CKで暗号化していたが、非特許文献1に記載のブロック暗号のモードを利用してもよい。例えば、CBCモードやOFB (Output Feedback) モード、CFB (Cipher Feedback) モードでもよく、さらに、ある一定間隔毎にあるモード (例：CBCモード) の初期値を初期化するようにしたものでも良い。

【0056】

(10) 配布部1010

配布部1010は、暗号化部1009から入力された暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCCNTを可搬媒体11へ記録するものである。

<配布センタ10の動作>

以上で、配布センタ10の構成について説明を行ったが、ここでは配布センタ10の動作の一例について、図10に示すフローチャートの処理を行う。なお、配布センタ10の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【0057】

入力部1001は、外部から入力されたコンテンツCNTをコンテンツ鍵生成部1002へ出力し、コンテンツ鍵生成部1002は、コンテンツ鍵CKを生成し、コンテンツ鍵CK及びコンテンツCNTを暗号化鍵束生成部1004へ出力する（ステップS101）。

暗号化鍵束生成部1004は、コンテンツ鍵生成部1002からコンテンツ鍵CK及びコンテンツCNTを入力され、実行装置情報格納部1003にアクセスして複数の実行装置12が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成する。そして、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKをコンテンツ位置情報生成部1005へ出力する（ステップS102）。

【0058】

コンテンツ位置情報生成部1005、暗号化鍵束生成部1004から暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKを入力され、k個の代表部分コンテンツを選択し、そのk個の代表部分コンテンツに対応する特定情報を取得する。そして、その代表部分コンテンツと特定情報のk組を、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとあわせて、ヘッダ情報生成部1006へ出力する（ステップS103）。

【0059】

ヘッダ情報生成部1006は、コンテンツ位置情報生成部1005から、代表部分コンテンツと特定情報のk組と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、代表部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を計算する。そして、その中から特定情報識別子と特定情報だけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報POSと、特定情報識別子とハッシュ値とを含むヘッダ情報HEADを生成する。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを認証情報生成部1008へ出力する（ステップS104）。

【0060】

認証情報生成部1008は、ヘッダ情報生成部1006からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、認証情報生成情報格納部1007にアクセスして、認証情報生成情報GENAUTHを取得する。そして、ヘッダ情報HEADと認証情報生成情報GENAUTHとを用いて、ヘッダ情報HEADに対する認証情報AUTHを生成する。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとを暗号化部1009へ出力する（ステップS105）。

【0061】

暗号化部1009は、認証情報生成部1008からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとが入力される。そして、コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCNTを生成し、同様にコンテンツ鍵CKを基に、コンテンツ位置情報POSを暗号化し、暗号化コンテンツ位置情報ENCPOSを生成する。そして、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとを配布部1010へ出力する（ステップS106）。

【0062】

配布部1010は、暗号化部1009から入力された暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとを可搬媒体11へ記録する（ステップS107）。

以上が、不正コンテンツ検知システム1の構成要素である配布センタ10の構成と動作である。続いて、可搬媒体11の構成について説明を行う。

【0063】

<可搬媒体11の構成>

可搬媒体11は、例えば、DVD-ROMやCD-ROM等のような可搬媒体であり、図11に示すように、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとが配布センタ10によって記録されているものとする。

【0064】

以上が、不正コンテンツ検知システム1の構成要素である可搬媒体11の構成である。続いて、実行装置12の構成と動作について説明を行う。

<実行装置12の構成>

実行装置12は、図12に示すように、取得部121、デバイス鍵格納部122、コンテンツ鍵取得部123、コンテンツ位置情報取得部124、検証情報格納部125、認証情報検証部126、部分復号化部127、ヘッダ情報検証部128、実行部129とから構成される。

【0065】

(1) 取得部121

取得部121は、可搬媒体11に記録されているデータの読み取りを行い、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとを受信する。そして、受信した暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとをコンテンツ鍵取得部123へ出力する。

【0066】

(2) デバイス鍵格納部122

デバイス鍵格納部122は、配布センタ10の実行装置情報格納部1003の中の鍵情報の一部を保持するものであり、このデバイス鍵格納部122に与えられる鍵情報と、暗号化鍵束KBを用いて、コンテンツ鍵CKが取得出来るものである。例えば、実行装置情報格納部1003が図3のような場合、デバイス鍵格納部122には、例として装置識別子AID_iとデバイス鍵K_i（iは1からnのいずれか）が与えられる。

【0067】

(3) コンテンツ鍵取得部123

コンテンツ鍵取得部123は、取得部121から暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとが入力された場合、デバイス鍵格納部122に格納されている鍵情報及び暗号化鍵束KBを用いて、コンテンツ鍵CKを取得する。例えば、暗号化鍵束KBが図5のような場合で、デバイス鍵格納部122には装置識別子AID_iとデバイス鍵DK_i（iは1からnのいずれか）が与えられている場合、コンテンツ鍵取得部123はデバイス鍵格納部122から装置識別子AID_iとデバイス鍵DK_iを取得し、暗号化鍵束KBの中から装置識別子AID_iに対応する暗号化コンテンツ鍵ENCCK_iを取得し、デバイス鍵DK_iを基に、暗号化コンテンツ鍵ENCCK_iを復号化することによって、コンテンツ鍵CKを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとをコンテンツ位置情報取得部124へ出力する。

【0068】

(4) コンテンツ位置情報取得部124

コンテンツ位置情報取得部124は、コンテンツ鍵取得部123からコンテンツ鍵CKとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとが入力された場合、コンテンツ鍵CKを基に、暗号化コンテンツ位置情報ENCPOSを復号化し、コンテンツ位置情報POSを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとを認証情報検証部126へ出力する。

【0069】

(5) 検証情報格納部125

検証情報格納部125は、ヘッダ情報HEADに対する認証情報AUTHの正当性を検証するために必要な検証情報VERを保持するものである。この検証情報VERに対応する認証情報生成情報GENAUTHは、配布センタ10の認証情報生成情報格納部1007に格納されている。例えば、検証情報VERはデジタル署名アルゴリズムの署名検証鍵である。

【0070】

(6) 認証情報検証部126

認証情報検証部126は、コンテンツ位置情報取得部124からコンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとが入力された場合、認証情報AUTHが発行センタ10によるヘッダ情報HEADの正しい認証情報であるかを検証する。例えば、以下のような流れで検証する。まず、検証情報格納部125に格納されている検証情報VERを取得する。そして、デジタル署名検証アルゴリズムを用いて、認証情報AUTHがヘッダ情報HEADの正しいデジタル署名であるかを検証する。例えば、認証情報AUTHが、k個の特定情報識別子ADDRESS1、・・・、ADDRESSkとk個のハッシュ値HASH1、・・・、HASHkを連結した値に対する正規のデジタル署名であるかどうかを検証する。このデジタル署名検証アルゴリズムは、配布センタ10の認証情報生成部1008で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献1に記載のDSA方式などである。認証情報検証部126は、認証情報AUTHが発行センタ10によるヘッダ情報HEADの正しいデジタル署名である場合にのみ、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTを部分復号化部127へ出力する。

【0071】

(7) 部分復号化部127

部分復号化部127は、認証情報検証部126からコンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTとが入力された場合、以下の処理を行う。まず、コンテンツ位置情報POSの一組目の特定情報識別子ADDRESS1と特定情報ADDRESS1を抽出する。そして、暗号化コンテンツENCNTの中から特定情報ADDRESS1が特定する暗号化代表部分コンテンツP1-CNTを取得し、コンテンツ鍵CKを基に復号化を行い、代表部分コンテンツP1-CNTを取得する。続いて、コンテンツ位置情報POSの二組目以降の特定情報識別子ADDRESS2、・・・、ADDRESSkと特定情報ADDRESS2、・・・、ADDRESSkとを同様に抽出し、代表部分コンテンツP2-CNT、・・・、Pk-CNTを取得する。そして、ヘッダ情報HEADと暗号化コンテンツENCNTと、抽出されたk組の特定情報識別子ADDRESS1、・・・、ADDRESSkと代表部分コンテンツP1-CNT、・・・、Pk-CNTと、コンテンツ鍵CKと、をヘッダ情報検証部128へ出力する。なお、部分復号化部127で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式などであり、配布センタ10の暗号化部1009と同じ暗号アルゴリズムを用いる。

【0072】

(8) ヘッダ情報検証部128

ヘッダ情報検証部128は、部分復号化部127からヘッダ情報HEADとコンテンツCNTとk組の特定情報識別子ADDRESS1、・・・、ADDRESSkと代表部分コンテンツP1-CNT、・・・、Pk-CNTと、コンテンツ鍵CKと、が入力された場合、まず、一組目の特定情報識別子ADDRESS1と代表部分コンテンツP1-CNTに対して、以下の処理を行う。最初に、代表部分コンテンツP1-CNTに対して、そのハッシュ値Xを計算する。代表部分コンテンツのハッシュ値を求める方法としては、例えば、一方向性関数を用いる方法があり、非特許文献1に記載のSHA-1アルゴリズムやブロック暗号を用いたCBC-MACなどがあり、配布センタ10のヘッダ情報生成部100

8で用いる方法と同じものを用いる。そして、ヘッダ情報HEADの中の特定情報識別子ADDRESS1に対応するハッシュ値HASH1と計算されたハッシュ値Xが等しいかどうか確認する。もし、同じ値であれば、二組目以降の特定情報識別子と代表部分コンテンツに対しても、同様にしてハッシュ値を計算し、ヘッダ情報HEADの中の対応する特定情報識別子のハッシュ値と比較する。ここで、全組のハッシュ値が等しかった場合にのみ、ヘッダ情報検証部128は実行部129へ暗号化コンテンツENCNTとコンテンツ鍵CKと、を出力する。

【0073】

(9) 実行部129

実行部129は、ヘッダ情報検証部128から入力された暗号化コンテンツENCNTの中のc個の暗号化部分コンテンツENCNT-1、・・・、ENCNT-cを、コンテンツ鍵CKを基に逐次復号化を行って部分コンテンツを取得し、逐次その部分コンテンツを実行するものであり、例えばディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生する、別の可搬媒体や記録媒体にコンテンツデータを出力する、コンテンツデータを紙などに印刷するなどがある

<実行装置12の動作>

以上で、実行装置12の構成について説明を行ったが、ここで実行装置12の動作について、図13に示すフローチャートを用いて説明する。なお、実行装置12の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【0074】

取得部121は、可搬媒体11に記録されているデータの読み取りを行い、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとをコンテンツ鍵取得部123へ出力する。そして、コンテンツ鍵取得部123は、入力された暗号化鍵束KB及びデバイス鍵格納部122が保持している鍵情報を用いて、コンテンツ鍵CKを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとをコンテンツ位置情報取得部124へ出力する（ステップS121）。

【0075】

コンテンツ位置情報取得部124は、コンテンツ鍵取得部123からコンテンツ鍵CKとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENCNTとを入力された場合、コンテンツ鍵CKを基に暗号化コンテンツ位置情報ENCPOSを復号化し、コンテンツ位置情報POSを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとを認証情報検証部126へ出力する（ステップS122）。

【0076】

認証情報検証部126は、コンテンツ位置情報取得部124からコンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTを入力された場合、検証情報格納部125に格納されている検証情報VERを用いて、ヘッダ情報HEADに対する正しい認証情報AUTHであるかを検証する（ステップS123）。

【0077】

認証情報検証部126は、認証情報AUTHがヘッダ情報HEADに対する発行センタ10の正しい認証情報である場合にのみ、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTを部分復号化部127へ出力し、ステップS125へ進む。もし、認証情報AUTHがヘッダ情報HEADに対する正しい認証情報ではない場合、処理を終了する（ステップS124）。

【0078】

部分復号化部127は、認証情報検証部126からコンテンツ鍵CKとヘッダ情報HEAD

A Dとコンテンツ位置情報P O Sと暗号化コンテンツE N C C N Tとを入力される。そして、コンテンツ鍵C Kを基に、暗号化コンテンツE N C C N Tの中のk個の特定情報のそれぞれに対する暗号化代表部分コンテンツをそれぞれ復号化し、k個の代表部分コンテンツP 1—C N T、・・・、P k—C N Tを抽出する。そして、ヘッダ情報H E A Dと暗号化コンテンツE N C C N Tと、k組の特定情報識別子A D D R I D 1、・・・、A D D R I D kと代表部分コンテンツP 1—C N T、・・・、P k—C N Tと、コンテンツ鍵C Kと、をヘッダ情報検証部1 2 8へ出力する（ステップS 1 2 5）。

【0079】

ヘッダ情報検証部1 2 8は、部分復号化部1 2 7からヘッダ情報H E A Dと暗号化コンテンツE N C C N Tと、k組の特定情報識別子A D D R I D 1、・・・、A D D R I D kと代表部分コンテンツP 1—C N T、・・・、P k—C N Tと、コンテンツ鍵C Kと、を入力される。そして、各組の代表部分コンテンツに対して、そのハッシュ値を計算する（ステップS 1 2 6）。

【0080】

ヘッダ情報検証部1 2 8は、計算したハッシュ値と、ヘッダ情報H E A Dの中の特定情報識別子に対応するハッシュ値とが等しいかどうか確認し、もし、全てのハッシュ値が同じ値であれば、ヘッダ情報検証部1 2 8は実行部1 2 9へ暗号化コンテンツE N C C N Tとコンテンツ鍵C Kを出力し、ステップS 1 2 8へ進む。もし、一つでも値が一致しなければ、処理を終了する（ステップS 1 2 7）。

【0081】

実行部1 2 9は、ヘッダ情報検証部1 2 8から受け取った暗号化コンテンツE N C C N Tの中の暗号化部分コンテンツを、コンテンツ鍵を用いて逐次復号化し、その部分コンテンツを実行する（ステップS 1 2 8）。

以上が、不正コンテンツ検知システム1の構成要素である実行装置1 2の構成と動作である。尚、コンテンツ鍵取得部1 2 3、コンテンツ位置情報取得部1 2 4、認証情報検証部1 2 6等の各機能ブロックは典型的には集積回路であるL S Iとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0082】

ここでは、L S Iとしたが、集積度の違いにより、I C、システムL S I、スーパーL S I、ウルトラL S Iと呼称されることもある。

また、集積回路化の手法はL S Iに限るものではなく、専用回路又は汎用プロセサで実現してもよい。L S I製造後に、プログラムすることが可能なF P G A（F i e l d P r o g r a m m a b l e G a t e A r r a y）や、L S I内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してよい。

【0083】

さらには、半導体技術の進歩又は派生する別技術によりL S Iに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム1の効果＞

以上、不正コンテンツ検知システム1について実施の形態に基づいて説明したが、この不正コンテンツ検知システム1においては、配布センタ1 0が、暗号化されたコンテンツC N Tとともに、コンテンツC N Tの中の、コンテンツ位置情報P O Sが特定する代表部分コンテンツに対応するヘッダ情報H E A D、及び、ヘッダ情報に対する認証情報A U T H（例えばデジタル署名）、及び、暗号化されたコンテンツ位置情報P O Sである暗号化コンテンツ位置情報E N C P O Sを可搬媒体1 1に記録するようにして、実行装置1 2が、コンテンツC N Tの実行開始前に、認証情報A U T Hがヘッダ情報H E A Dに対する正規の認証情報（例えばデジタル署名）であるか検証するとともに、暗号化コンテンツ位置情報E N C P O Sを復号化してコンテンツ位置情報P O Sを取得し、ヘッダ情報H E A DがコンテンツC N Tの中のコンテンツ位置情報P O Sが特定する代表部分コンテンツに対

応する正規のヘッダ情報であるかを検証し、共に正当であると検証された場合にのみ、コンテンツＣＮＴの実行を開始するようにした。そうすることにより、実行装置１２は、不正な認証情報AUTHもしくはヘッダ情報HEADもしくはコンテンツＣＮＴが記録された可搬媒体１１のコンテンツＣＮＴは実行開始しないようになり、不正コンテンツの配布を防止することが出来るようになった。

【００８４】

さらに、コンテンツ位置情報POSは暗号化されて可搬媒体１１に記録されているため、不正者がコンテンツＣＮＴの中のコンテンツ位置情報POSが特定する代表部分コンテンツのみを差し替えようとする攻撃が適用不可能となる。また、実行装置１２は、認証情報AUTHの正当性の検証を、コンテンツＣＮＴを実行開始する前に全て行うため、コンテンツＣＮＴの実行中の特別な処理が必要なくなり、コンテンツＣＮＴの実行中の処理負荷が軽減されるという効果を有する。

【００８５】

（実施の形態２）

図１４は、本発明の実施の形態２の不正コンテンツ検知システムの構成図である。実施の形態２においては、実施の形態１と同様に、配布センタ２０は外部からコンテンツＣＮＴを受け取り、後述する実行装置２２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体２１に記録するものであり、可搬媒体２１はコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置２２は可搬媒体２１に記録されている情報を基にコンテンツＣＮＴを実行するものである。

【００８６】

実施の形態１では、可搬媒体１１はヘッダ情報と暗号化コンテンツ位置情報と認証情報とを１種類ずつ含んでいたが、実施の形態２での可搬媒体２１では、ヘッダ情報と暗号化コンテンツ位置情報と認証情報とをそれぞれ複数種類含んでいる点が異なる。そして、各実行装置２２は、可搬媒体２１からその一部のヘッダ情報と暗号化コンテンツ位置情報と認証情報とを選択し、その選択したヘッダ情報と暗号化コンテンツ位置情報と認証情報のみを検証する点が実施の形態１と異なる。

【００８７】

以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム２の詳細について説明を行う。

＜不正コンテンツ検知システム２の構成＞

不正コンテンツ検知システム２は、図１４に示すように、配布センタ２０と、可搬媒体２１と、複数の実行装置２２から構成される。

【００８８】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ２０の構成と動作について述べ、続いて可搬媒体２１の構成について述べ、最後に実行装置２２の構成と動作について述べる。

＜配布センタ２０の構成＞

配布センタ２０は、図１５に示すように、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、コンテンツ位置情報生成部２００５、ヘッダ情報生成部２００６、認証情報生成情報格納部１００７、認証情報生成部２００８、暗号化部２００９、配布部２０１０から構成される。なお、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、認証情報生成情報格納部１００７については、実施の形態１の配布センタ１０と同じ構成要素であるため、説明を省略する。

【００８９】

（１）コンテンツ位置情報生成部２００５

コンテンツ位置情報生成部２００５において、実施の形態１のコンテンツ位置情報生成部１００５と異なる点についてのみ説明する。コンテンツ位置情報生成部１００５では、 k 個の代表部分コンテンツと k 個の特定情報をそれぞれ１種類のみ作成していたが、コン

テンツ位置情報生成部2005においては、k個の代表部分コンテンツとk個の特定情報をそれぞれm種類作成する点異なる。そのm種類をそれぞれ{ {P1-1-CNT、ADDR1-1}、{P2-1-CNT、ADDR2-1}、・・・、{Pk-1-CNT、ADDRk-1} }、{ {P1-2-CNT、ADDR1-2}、{P2-2-CNT、ADDR2-2}、・・・、{Pk-2-CNT、ADDRk-2} }、・・・、{ {P1-m-CNT、ADDR1-m}、{P2-m-CNT、ADDR2-m}、・・・、{Pk-m-CNT、ADDRk-m} }とする。そして、m種類それぞれに対して、ヘッダ識別子HEADID1、・・・、HEADIDmを生成し、それぞれに対応づける。ヘッダ識別子を生成する方法としては、自然数を順番に割り当てていく(1、2、3、・・・、m)方法や、乱数を用いる方法などがある。その状態を、{HEADID1、{P1-1-CNT、ADDR1-1}、{P2-1-CNT、ADDR2-1}、・・・、{Pk-1-CNT、ADDRk-1} }、{HEADID2、{P1-2-CNT、ADDR1-2}、{P2-2-CNT、ADDR2-2}、・・・、{Pk-2-CNT、ADDRk-2} }、・・・、{HEADIDm、{P1-m-CNT、ADDR1-m}、{P2-m-CNT、ADDR2-m}、・・・、{Pk-m-CNT、ADDRk-m} }とする。そして、ヘッダ識別子とk個の代表部分コンテンツとk個の特定情報をそれぞれm種類と、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとをあわせて、ヘッダ情報生成部2006へ出力する。mは例えば10であるが、2以上の自然数であればどのような値でも良い。

【0090】

(2) ヘッダ情報生成部2006

ヘッダ情報生成部2006において、実施の形態1のヘッダ情報生成部1006と異なる点についてのみ説明する。ヘッダ情報生成部1006では、k個の代表部分コンテンツとk個の特定情報の1種類に対してのみヘッダ情報を作成していたが、ヘッダ情報生成部2006においては、k個のヘッダ情報識別子とk個の代表部分コンテンツとk個の特定情報のm種類それぞれに対して、ヘッダ情報を作成(ヘッダ情報をm個)する点異なる。それぞれのヘッダ情報を作成する方法は、実施の形態1のヘッダ情報生成部1006と同じ方法である。まず実施の形態1のヘッダ情報生成部1006と同様に、各代表部分コンテンツに対して、特定情報識別子とハッシュ値を作成した結果を以下のように表記する。{HEADID1、{ADDRID1-1、P1-1-CNT、ADDR1-1、HASH1-1}、{ADDRID2-1、P2-1-CNT、ADDR2-1、HASH2-1}、・・・、{ADDRIDk-1、Pk-1-CNT、ADDRk-1、HASHk-1} }、{HEADID2、{ADDRID1-2、P1-2-CNT、ADDR1-2、HASH1-2}、{ADDRID2-2、P2-2-CNT、ADDR2-2、HASH2-2}、・・・、{ADDRIDk-2、Pk-2-CNT、ADDRk-2、HASHk-2} }、・・・、{HEADIDm、{ADDRID1-m、P1-m-CNT、ADDR1-m、HASH1-m}、{ADDRID2-m、P2-m-CNT、ADDR2-m、HASH2-m}、・・・、{ADDRIDk-m、Pk-m-CNT、ADDRk-m、HASHk-m} }。そして、実施の形態1のヘッダ情報生成部1006と同様の処理に、その中から、ヘッダ識別子と特定情報識別子と特定情報だけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報をm種類(POS-1、・・・、POS-m)それぞれヘッダ識別子(HEADID1、・・・、HEADIDm)と対応づけて生成する。また、同様にその中から、ヘッダ識別子と特定情報識別子とハッシュ値だけを抽出し、特定情報識別子とハッシュ値とを含むm種類のヘッダ情報(HEAD-1、・・・、HEAD-m)をヘッダ識別子(HEADID1、・・・、HEADIDm)と対応付けて生成する。そして、m種類のヘッダ識別子(HEADID1、・・・、HEADIDm)とm種類のコンテンツ位置情報(POS1、・・・、POSm)とm種類のヘッダ情報(HEAD1、・・・、HEADm)と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを認証情報生成部2008へ出力する。

【0091】

(3) 認証情報生成部2008

認証情報生成部2008において、実施の形態1の認証情報生成部1008と異なる点についてのみ説明する。認証情報生成部1008では、1つのヘッダ情報に対してのみ認証情報を作成していたが、認証情報生成部2008においては、m種類のヘッダ情報(HEAD1、・・・、HEADm)のそれぞれに対して、m種類の認証情報(AUTH1、・・・、AUTHm)を作成する点が異なる。そして、m種類のヘッダ識別子(HEADID1、・・・、HEADIDm)とm種類のコンテンツ位置情報(POS1、・・・、POSm)とm種類のヘッダ情報(HEAD1、・・・、HEADm)とm種類の認証情報(AUTH1、・・・、AUTHm)と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを暗号化部2009へ出力する。

【0092】

(4) 暗号化部2009

暗号化部2009において、実施の形態1の暗号化部1009と異なる点についてのみ説明する。暗号化部1009では、1つのコンテンツ位置情報に対してのみ暗号化を行っていたが、暗号化部2009においては、m種類のコンテンツ位置情報(POS1、・・・、POSm)のそれぞれに対して暗号化を行い、m種類の暗号化コンテンツ位置情報(ENCPOS1、・・・、ENCPOSm)を作成する点が異なる。そして、m種類のヘッダ識別子(HEADID1、・・・、HEADIDm)とm種類のヘッダ情報(HEAD1、・・・、HEADm)とm種類の暗号化コンテンツ位置情報(ENCPOS1、・・・、ENCPOSm)とm種類の認証情報(AUTH1、・・・、AUTHm)と暗号化鍵束KBと暗号化コンテンツENCCNTを配布部2010へ出力する。

【0093】

(5) 配布部2010

配布部2010は、暗号化部2009から入力されたm種類のヘッダ識別子(HEADID1、・・・、HEADIDm)とm種類のヘッダ情報(HEAD1、・・・、HEADm)とm種類の暗号化コンテンツ位置情報(ENCPOS1、・・・、ENCPOSm)とm種類の認証情報(AUTH1、・・・、AUTHm)と暗号化鍵束KBと暗号化コンテンツENCCNTとを可搬媒体21へ記録する。

【0094】

<配布センタ20の動作>

以上で、配布センタ20の構成について説明を行ったが、ここでは配布センタ20の動作の一例について、図16に示すフローチャートの処理を行う。なお、配布センタ20の動作に関しても、配布センタ10同様、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【0095】

ステップS101と同じ動作であるため、説明を省略する(ステップS201)。

ステップS102と同じ動作であるため、説明を省略する(ステップS202)。

コンテンツ位置情報生成部2005は、暗号化鍵束生成部1004から暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、m種類のヘッダ識別子(HEADID1、・・・、HEADIDm)を生成する。そして、k個の代表部分コンテンツをm種類選択し、各代表部分コンテンツに対応する特定情報を取得する。そして、k個の代表部分コンテンツとk個の特定情報のm種類それぞれをヘッダ識別子と対応づけて、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとあわせて、ヘッダ情報生成部2006へ出力する(ステップS203)。

【0096】

ヘッダ情報生成部2006は、コンテンツ位置情報生成部2005から、m種類のヘッダ識別子(HEADID1、・・・、HEADIDm)と、k組の代表部分コンテンツと特定情報をm種類と、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、特定情報の各々に対して、特定情報識別子を生成する。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を

計算する。そして、その中から特定情報識別子と特定情報とだけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報をm種類と、特定情報識別子とハッシュ値とを含むヘッダ情報をm種類を、それぞれヘッダ識別子と対応づけて生成する。そして、m種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のコンテンツ位置情報（POS1、・・・、POSm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを認証情報生成部2008へ出力する（ステップS204）。

【0097】

認証情報生成部2008は、ヘッダ情報生成部2006からm種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のコンテンツ位置情報（POS1、・・・、POSm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、認証情報生成情報格納部1007にアクセスして、認証情報生成情報GENAUTHを取得する。そして、m種類のヘッダ情報HEAD1、・・・、HEADmと認証情報生成情報GENAUTHとを基に、m種類の認証情報AUTH1、・・・、AUTHmをそれぞれ生成する。そして、m種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のコンテンツ位置情報（POSID1、・・・、POSIDm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）とm種類の認証情報（AUTH1、・・・、AUTHm）と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを暗号化部2009へ出力する（ステップS205）。

【0098】

暗号化部2009は、認証情報生成部2008からm種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のコンテンツ位置情報（POSID1、・・・、POSIDm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）とm種類の認証情報（AUTH1、・・・、AUTHm）と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力される。そして、コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCNTを生成し、同様にコンテンツ鍵CKを基に、m種類のコンテンツ位置情報POS1、・・・、POSmを暗号化し、m種類の暗号化コンテンツ位置情報ENCPOS1、・・・、ENCPOSmを生成する。そして、暗号化鍵束KBとm種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）とm種類の暗号化コンテンツ位置情報（ENCPOSID1、・・・、ENCPOSIDm）とm種類の認証情報（AUTH1、・・・、AUTHm）と暗号化コンテンツENCNTとを配布部2010へ出力する（ステップS206）。

【0099】

配布部2010は、暗号化部2009から入力された暗号化鍵束KBとm種類のヘッダ識別子（HEADID1、・・・、HEADIDm）とm種類のヘッダ情報（HEAD1、・・・、HEADm）とm種類の暗号化コンテンツ位置情報（ENCPOSID1、・・・、ENCPOSIDm）とm種類の認証情報（AUTH1、・・・、AUTHm）と暗号化コンテンツENCNTとを可搬媒体21へ記録する（ステップS207）。

【0100】

以上が、不正コンテンツ検知システム2の構成要素である配布センタ20の構成と動作である。続いて、可搬媒体21の構成について説明を行う。

＜可搬媒体21の構成＞

可搬媒体21は、例えば、DVD-ROMやCD-ROM等のような可搬媒体であり、図17に示すように、暗号化鍵束KBとm種類のヘッダ識別子HEADID1、・・・、HEADIDmとm種類のヘッダ情報HEAD1、・・・、HEADmとm種類の暗号化コンテンツ位置情報ENCPOS1、・・・、ENCPOSmとm種類の認証情報AUTH1、・・・、AUTHmと暗号化コンテンツENCNTとが、配布センタ20によって記録されているものである。

【0101】

以上が、不正コンテンツ検知システム2の構成要素である可搬媒体21の構成である。続いて、実行装置22の構成と動作について説明を行う。

<実行装置22の構成>

実行装置22は、図18に示すように、取得部221、デバイス鍵格納部122、コンテンツ鍵取得部123、コンテンツ位置情報取得部124、検証情報格納部125、認証情報検証部126、部分復号化部127、ヘッダ情報検証部128、実行部129とから構成される。なお、デバイス鍵格納部122、コンテンツ鍵取得部123、コンテンツ位置情報取得部124、検証情報格納部125、認証情報検証部126、部分復号化部127、ヘッダ情報検証部128、実行部129については、実施の形態1の実行装置12と同じ構成要素であるため、説明を省略する。

【0102】

(1) 取得部221

取得部221は、まず、m種類のヘッダ識別子HEADID1、・・・、HEADIDmの中から一種類のヘッダ識別子を選択する。m種類のヘッダ識別子HEADID1、・・・、HEADIDmから一種類のヘッダ識別子を選択する方法は、乱数を用いてランダムに選択する方法や、前回選択したヘッダ識別子を記憶しておくことによってHEADID1から順番に一つ一つ選択していく方法などがある。ここでは、HEADIDi (HEADIDiはHEADID1、・・・、HEADIDmのいずれか)を選択したとする。そして、可搬媒体21に記録されているデータの読み取りを行い、暗号化鍵束KBとヘッダ識別子HEADIDiに対応するヘッダ情報HEADi (HEADiはHEAD1、・・・、HEADmのいずれか)と暗号化コンテンツ位置情報ENCPOSi (ENCPOSiはENCPOS1、・・・、ENCPOSmのいずれか)と認証情報AUTHi (AUTHiはAUTH1、・・・、AUTHmのいずれか)と暗号化コンテンツENC CNTを取得する。そして、その取得したヘッダ情報HEADiと暗号化コンテンツ位置情報ENCPOSiと認証情報AUTHiをそれぞれ、ヘッダ情報HEAD、暗号化コンテンツ位置情報ENCPOS、認証情報AUTH、とする。そして、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENC CNTをコンテンツ鍵取得部123へ出力する。

【0103】

<実行装置22の動作>

以上で、実行装置22の構成について説明を行ったが、ここで実行装置22の動作について、図19に示すフローチャートを用いて説明する。なお、実行装置22の動作に関しても、実行装置12同様、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【0104】

取得部221は、まず、m種類のヘッダ識別子HEADID1、・・・、HEADIDmから一種類のヘッダ識別子を選択する。ここでは、HEADIDi (HEADIDiはHEAD1、・・・、HEADmのいずれか)を選択したとする。そして、可搬媒体21に記録されているデータの読み取りを行った、暗号化鍵束KBとヘッダ情報HEADiと暗号化コンテンツ位置情報ENCPOSiと認証情報AUTHiと暗号化コンテンツENC CNTを、暗号化鍵束KBとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENC CNTとして、コンテンツ鍵取得部123へ出力する。そして、コンテンツ鍵取得部123は、入力された暗号化鍵束KB、及び、デバイス鍵格納部122に格納されている鍵情報を用いて、コンテンツ鍵CKを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADと暗号化コンテンツ位置情報ENCPOSと認証情報AUTHと暗号化コンテンツENC CNTをコンテンツ位置情報取得部124へ出力する(ステップS221)。

【0105】

ステップS122と同じ動作であるので、説明を省略する(ステップS222)。

ステップS 1 2 3と同じ動作であるので、説明を省略する（ステップS 2 2 3）。

ステップS 1 2 4と同じ動作であるので、説明を省略する（ステップS 2 2 4）。

ステップS 1 2 5と同じ動作であるので、説明を省略する（ステップS 2 2 5）。

ステップS 1 2 6と同じ動作であるので、説明を省略する（ステップS 2 2 6）。

【0106】

ステップS 1 2 7と同じ動作であるので、説明を省略する（ステップS 2 2 7）。

ステップS 1 2 8と同じ動作であるので、説明を省略する（ステップS 2 2 8）。

以上が、不正コンテンツ検知システム2の構成要素である実行装置22の構成と動作である。尚、コンテンツ鍵取得部123、コンテンツ位置情報取得部124、認証情報検証部126等の各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0107】

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA（Field Programmable Gate Array）や、LSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

【0108】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム2の効果＞

以上で、不正コンテンツ検知システム2について実施の形態に基づいて説明を行った。この不正コンテンツ検知システム2は、基本的に不正コンテンツ検知システム1と同様の効果を有するが、配布センタ20が、一つのコンテンツCNTに対し、複数の認証情報を可搬媒体21に記録するようにして、実行装置22が、コンテンツCNTの実行開始前に、複数の認証情報のいずれかの認証情報の正当性を検証し、それが正当な場合にのみ、コンテンツCNTの実行を開始するようにした。つまり、複数の認証情報が可搬媒体21に記録されているため、不正コンテンツ検知システム1に比べて、不正者による認証情報の偽造がより困難となり、安全性をより向上させることが出来るという効果を有する。

【0109】

（実施の形態3）

図20は、本発明の実施の形態3における不正コンテンツ検知システムの構成図である。図20において、配布センタ30は外部からコンテンツCNTを受け取り、後述する実行装置32がコンテンツCNTを実行するために必要となる情報を後述する可搬媒体31に記録するものであり、可搬媒体31は実行装置32がコンテンツCNTを実行するために必要となる情報が記録されているものであり、複数の実行装置32は可搬媒体31に記録されている情報を用いて、コンテンツCNTを実行するものである。

【0110】

不正コンテンツ検知システム3は、配布センタ30（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、DVD（Digital Versatile Disc）等の可搬媒体31の配布手段によって、暗号化されたコンテンツCNTである暗号化コンテンツENCNTと、コンテンツCNTを基に生成されるヘッダ情報HEADと、ヘッダ情報HEADの正当性を示す情報である認証情報AUTHを、各実行装置32へ配布する。各実行装置32は、暗号化コンテンツENCNTを復号化してコンテンツCNTを取得し、認証情報AUTHが配布センタ30によるヘッダ情報HEADの正規の認証情報であることと、ヘッダ情報HEADがコンテンツCNTを基に生成されたものであることを確認し、コンテンツCNTを実行開始する。

【0111】

以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム3の詳細について説明を行う。

＜不正コンテンツ検知システム3の構成＞

不正コンテンツ検知システム3は、図20に示すように、配布センタ30と、可搬媒体31と、n個の実行装置32（nは1以上の自然数）から構成される。

【0112】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ30の構成と動作について述べ、続いて可搬媒体31の構成について述べ、最後に実行装置32の構成と動作について述べる。

＜配布センタ30の構成＞

配布センタ30は、図21に示すように、入力部3001、コンテンツ鍵生成部3002、実行装置情報格納部3003、暗号化鍵束生成部3004、コンテンツ位置情報生成部3005、ヘッダ情報生成部3006、認証情報生成情報格納部3007、認証情報生成部3008、暗号化部3009、配布部3010から構成される。

【0113】

（1）入力部3001

入力部3001は、外部からコンテンツCNTを入力出来るものである。入力部3001は、例えば、可搬媒体であるDVD-ROM等からコンテンツCNTを読み取る機能を有する。外部から入力されるコンテンツCNTは、実行装置32で実行可能なフォーマット形式であって、例えば、MPEG（Moving Picture Experts Group）2フォーマット形式による動画データやMP3フォーマットによる音声データなどである。外部からコンテンツCNTが入力された場合、そのコンテンツCNTをコンテンツ鍵生成部3002へ出力する。

【0114】

（2）コンテンツ鍵生成部3002

コンテンツ鍵生成部3002は、入力部3001からコンテンツCNTが入力された場合、コンテンツ鍵CKを生成する。コンテンツ鍵CKを生成する方法としては、例えば、乱数を用いて128ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部3002が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献2が詳しい。そして、コンテンツ鍵CK及びコンテンツCNTを暗号化鍵束生成部3004へ出力する。なお、コンテンツ鍵CKはコンテンツCNTを暗号化、復号化するための鍵であり、暗号化部3009及び実行装置32の部分復号化部327で使用される。

【0115】

（3）実行装置情報格納部3003

実行装置情報格納部3003は、複数の実行装置32に与えられる鍵情報を保持するものである。図22は、実行装置情報格納部3003の一例を示しており、装置識別子AID1に対応付けられたデバイス鍵DK1と、装置識別子AID2に対応付けられたデバイス鍵DK2と、・・・、装置識別子AIDnに対応付けられたデバイス鍵DKnを保持している状態を示している。ここで、装置識別子AID1、AID2、・・・、AIDnのそれぞれは、複数の実行装置32のいずれかに対応付けられており、デバイス鍵DK1、DK2、・・・、DKnのそれぞれは、対応する実行装置32のデバイス鍵格納部322に格納されている鍵である。なお、デバイス鍵DK1、DK2、・・・、DKnのそれぞれはコンテンツ鍵CKを暗号化、復号化するための鍵であり、暗号化鍵束生成部3004及びコンテンツ鍵取得部323で用いられる。例えば、装置識別子AID1、AID2、・・・、AIDnは、それぞれ異なる自然数1、2、・・・、nであり、デバイス鍵DK1、DK2、・・・、DKnは、例えば、それぞれ異なる128ビット鍵データである。

【0116】

（4）暗号化鍵束生成部3004

暗号化鍵束生成部3004は、コンテンツ鍵生成部3002からコンテンツ鍵CK及びコンテンツCNTが入力された場合、実行装置情報格納部3003にアクセスして複数の実行装置32が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成する。暗号化鍵束KBは、各実行装置32がその暗号化鍵束KBと自身の保持する鍵を用いてコンテンツ鍵CKが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置32はそれぞれ、AID1からAIDnのいずれかの装置識別子と対応するデバイス鍵(DK1、・・・、DKn)を保持しており、実行装置情報格納部3003には、図22のように、実行装置32が保持する装置識別子(AID1、・・・、AIDn)と対応するデバイス鍵(DK1、・・・、DKn)の組が全て格納されているとする。そのような場合、暗号化鍵束KBは例えば以下のように生成される。実行装置情報格納部3003から装置識別子AID1と対応するデバイス鍵DK1を取得する。そして、デバイス鍵DK1を基にコンテンツ鍵CKを暗号化し、暗号化コンテンツ鍵ENCCK1=Enc(DK1、CK)を生成し、装置識別子AID1に対応付ける。なお、Enc(K、P)を平文Pを暗号化鍵Kで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子(AID2、・・・、AIDn)とデバイス鍵(DK2、・・・、DKn)に対しても同様の処理を行い、暗号化コンテンツ鍵ENCCK2=Enc(DK2、CK)、・・・、ENCCKn=Enc(DKn、CK)を生成し、装置識別子AID2、・・・、AIDnに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のn組から構成される、図23のような暗号化鍵束KBを生成する。暗号化鍵束KBをこのような構成にすることによって、各実行装置32はその暗号化鍵束KBと自身の保持するデバイス鍵(DK1、・・・、DKnの何れか)を用いてコンテンツ鍵CKが取得出来るようになる。そして、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKをコンテンツ位置情報生成部3005に出力する。なお、特許文献2などに記載の方法を用いることで、暗号化鍵束KBの中の暗号化コンテンツ鍵(先程の例ではn個)の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵CKを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部3004で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式(128ビット鍵)などであり、実行装置32のコンテンツ鍵取得部323と同じ暗号アルゴリズムを用いる。

【0117】

(5) コンテンツ位置情報生成部3005

コンテンツ位置情報生成部3005は、暗号化鍵束生成部3004から暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力される。そして、まずコンテンツCNTを、図24で示すようにc個(cは2以上の自然数)の部分コンテンツCNT-1、CNT-2、CNT-3、・・・、CNT-a、・・・、CNT-cに分割する。コンテンツCNTをc個に分割する方法は、例えばコンテンツデータのある所定の区切り毎に分割する方法がある。ある所定の区切りの具体例としては、コンテンツデータがDVD-VIDEO形式の動画コンテンツの場合、例えば、VOB(Video Object)ファイル単位や、VOB単位や、VOBU(Video Object Unit)単位、セル(Cell)単位などである。コンテンツデータがMPEG2形式の動画コンテンツの場合、例えば、GOP単位、フィールド単位、フレーム単位、Iピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、トラック単位、シリンダ単位などである。また、コンテンツデータの形式を問わず、例えば、64キロバイト単位、1メガバイト単位、1秒単位、1分単位などでも良い。なお、DVD-Video形式については、例えば<http://positron.jfet.org/dvdvideo.html>に記載されており、MPEG形式については、例えば<http://www.pioneer.co.jp/crdl/tech/mpeg/1.html>に記載されている。そして、c個に分割された部分コンテンツのそれぞれを識別、特定出来る、c個の特定情報ADDR1、・・・、ADDRcを取得する。このc個の特定情報の取得方法としては、例えば、所定の方法で区切った部分コンテンツに対して順番に番号(例えば1、2、・・・、c)を付けていく方法や、部分コンテンツの先頭を表すアドレス

(物理アドレスや論理アドレスなど)と部分コンテンツのサイズを計算する方法や、コンテンツの先頭からの経過時間を計算する方法などがある。ここでは、部分コンテンツCNT-1を識別、特定する情報を特定情報ADDR1、部分コンテンツCNT-2を識別、特定する情報を特定情報ADDR2、部分コンテンツCNT-3を識別、特定する情報を特定情報ADDR3、・・・、部分コンテンツCNT-aを特定する情報を特定情報ADDRa、・・・、部分コンテンツCNT-cを特定する情報を特定情報ADDRcとする。そして、部分コンテンツと特定情報のc組{CNT-1、ADDR1}、{CNT-2、ADDR2}、・・・、{CNT-a、ADDRa}、・・・、{CNT-c、ADDRc}を、暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKと併せて、ヘッダ情報生成部3006へ出力する。

【0118】

なお、例えば、コンテンツCNTが2時間の動画データで各部分コンテンツが1秒の動画データの場合、cは7200となるが、cは2以上の自然数であればどのような値でも良い。さらに、それぞれの特定情報は、上記で紹介した情報に限らず、各部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。さらには、上記情報を複数組み合わせた情報であっても良い。

【0119】

(6) ヘッダ情報生成部3006

ヘッダ情報生成部3006は、コンテンツ位置情報生成部3005から、部分コンテンツと特定情報のc組{CNT-1、ADDR1}、{CNT-2、ADDR2}、・・・、{CNT-a、ADDRa}、・・・、{CNT-c、ADDRc}と暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとが入力された場合、以下のようにして、ヘッダ情報HEADを生成する。まず、c組の部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。特定情報識別子を生成する方法としては、自然数を順番に割り当てていく(1、2、・・・、c)方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した特定情報識別子をそれぞれ、ADDRID1、ADDRID2、・・・、ADDRIDa、・・・、ADDRIDcとし、次のように特定情報識別子と部分コンテンツと特定情報とが対応しているとする。{ADDRID1、CNT-1、ADDR1}、{ADDRID2、CNT-2、ADDR2}、・・・、{ADDRIDa、CNT-a、ADDRa}、・・・、{ADDRIDc、CNT-c、ADDRc}。続いて、c組の特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値としてハッシュ値を計算する。部分コンテンツのハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献1に記載のSHA-1アルゴリズムやブロック暗号を用いたCBC-MACなどがあり、実行装置32のヘッダ情報検証部328で用いる方法と同じものを用いる。ここで、各組に対して計算したハッシュ値をそれぞれ、HASH1、HASH2、・・・、HASHa、・・・、HASHcとし、次のように特定情報識別子と部分コンテンツと特定情報とハッシュ値が対応しているとする。{ADDRID1、CNT-1、ADDR1、HASH1}、{ADDRID2、CNT-2、ADDR2、HASH2}、・・・、{ADDRIDa、CNT-a、ADDRa、HASHa}、・・・、{ADDRIDc、CNT-c、ADDRc、HASHc}。そして、その中から特定情報識別子と特定情報だけを抽出し、図25で示すような、特定情報識別子と特定情報とからなるコンテンツ位置情報POS={ADDRID1、ADDR1}、{ADDRID2、ADDR2}、・・・、{ADDRIDa、ADDRa}、・・・、{ADDRIDc、ADDRc}を生成する。また、特定情報識別子とハッシュ値だけを抽出し、図26で示すような、特定情報識別子とハッシュ値とからなるヘッダ情報HEAD={ADDRID1、HASH1}、{ADDRID2、HASH2}、・・・、{ADDRIDa、HASHa}、・・・、{ADDRIDc、HASHc}を生成する。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKとを認証情報生成部3008へ出力する。

【0120】

(7) 認証情報生成情報格納部3007

認証情報生成情報格納部3007は、ヘッダ情報HEADの認証情報である認証情報AUTHを生成するための、認証情報生成情報GENAUTHを保持するものである。この認証情報生成情報GENAUTHは、例えば、デジタル署名アルゴリズムの署名生成鍵（秘密鍵）である。認証情報生成情報GENAUTHに対応する検証情報VERは、実行装置32の検証情報格納部325に格納されている。この検証情報VERは、例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デジタル署名アルゴリズムは、例えば、非特許文献1に記載のDSA方式などである。

【0121】

(8) 認証情報生成部3008

認証情報生成部3008は、ヘッダ情報生成部3006からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBとコンテンツCNTとコンテンツ鍵CKが入力された場合、以下のようにして、ヘッダ情報HEADに対する認証情報AUTHを生成する。まず、認証情報生成情報格納部3007にアクセスして、認証情報生成情報GENAUTHを取得する。そして、ヘッダ情報HEADと認証情報生成情報GENAUTHを用いて、ヘッダ情報HEADの認証情報である認証情報AUTHを生成する。なお、認証情報AUTHの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。具体的には、例えば非特許文献1に記載のDSA方式などを用い、ヘッダ情報HEADのc個全てのハッシュ値HASH1、HASH2、・・・、HASHa、・・・、HASHcを結合した値HASH1||HASH2||・・・||HASHa||・・・||HASHcに対するデジタル署名を作成する。ここで、GENSIG(K、M)を署名生成鍵Kを用いてメッセージMに対して生成されたデジタル署名とすると、認証情報AUTHは、AUTH=GENSIG(GENAUTH、HASH1||HASH2||・・・||HASHa||・・・||HASHc)となる。そして、コンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとを暗号化部3009へ出力する。なお、認証情報生成部3008で使用するデジタル署名アルゴリズムは、実行装置32のヘッダ情報検証部328で用いるデジタル署名アルゴリズムと同じものを用いる。

【0122】

(9) 暗号化部3009

暗号化部3009は、認証情報生成部3008からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとが入力された場合、以下のようにして暗号化コンテンツENCCNTを生成する。コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCCNTを生成する。この暗号化コンテンツENCCNTの生成方法としては、例えば、以下のような方法がある。まず、コンテンツ鍵CKを用いて部分コンテンツCNT-1を暗号化し、暗号化部分コンテンツENCCNT-1=Enc(CK、CNT-1)を生成する。続いて、同じコンテンツ鍵CKを用いて部分コンテンツCNT-2を暗号化し、暗号化部分コンテンツENCCNT-2=Enc(CK、CNT-2)を生成する。これを繰り返して、図27で示すようなc個の暗号化部分コンテンツENCCNT-1、・・・、ENCCNT-a、・・・、ENCCNT-cから構成される暗号化コンテンツENCCNTを生成する。そして、暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTを配布部3010へ出力する。暗号化部3009で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のAES方式（128ビット鍵）などであり、実行装置32の部分復号化部327と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツENCCNTの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵CKで暗号化していたが、非特許文献1に記載のブロック暗号のモードを利用してよい。例えば、CBCモードやOFBモード、CFBモードなどでもよく、さらに、ある一定間隔毎にモード（例：CBCモード）の初期値を変化させるようにしたものでも良い。さらに、暗号化を行う単位は、コンテンツ位置情報生成

部 3 0 0 5 でコンテンツ C N T を分割した単位に限るものではなく、例えば 1 6 バイト毎であっても良い。

【 0 1 2 3 】

(1 0) 配布部 3 0 1 0

配布部 3 0 1 0 は、暗号化部 3 0 0 9 から入力された暗号化鍵束 K B とヘッダ情報 H E A D とコンテンツ位置情報 P O S と認証情報 A U T H と暗号化コンテンツ E N C C N T を可搬媒体 3 1 へ記録するものである。例えば、可搬媒体 3 1 が書き込み可能な光ディスクであり、配布部 3 0 1 0 は書き込み用レーザー等を用いてデータを記録する。

【 0 1 2 4 】

＜配布センタ 3 0 の動作＞

以上で、配布センタ 3 0 の構成について説明を行ったが、ここでは配布センタ 3 0 の動作の一例について、図 2 8 に示すフローチャートの処理を行う。なお、配布センタ 3 0 の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【 0 1 2 5 】

入力部 3 0 0 1 は、外部から入力されたコンテンツ C N T をコンテンツ鍵生成部 3 0 0 2 へ出力し、コンテンツ鍵生成部 3 0 0 2 は、コンテンツ鍵 C K を生成し、コンテンツ鍵 C K 及びコンテンツ C N T を暗号化鍵束生成部 3 0 0 4 へ出力する（ステップ S 3 0 1 ）。

暗号化鍵束生成部 3 0 0 4 は、コンテンツ鍵生成部 3 0 0 2 からコンテンツ鍵 C K 及びコンテンツ C N T を入力され、実行装置情報格納部 3 0 0 3 にアクセスして複数の実行装置 3 2 が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵 C K とを基に、暗号化鍵束 K B を生成する。そして、暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K をコンテンツ位置情報生成部 3 0 0 5 に出力する（ステップ S 3 0 2 ）。

【 0 1 2 6 】

コンテンツ位置情報生成部 3 0 0 5 、暗号化鍵束生成部 3 0 0 4 から暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K を入力され、コンテンツ C N T を c 個の部分コンテンツに分割し、その c 個の部分コンテンツのそれぞれを識別、特定する c 個の特定情報を取得する。そして、c 組の部分コンテンツと特定情報を、暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K とあわせて、ヘッダ情報生成部 3 0 0 6 へ出力する（ステップ S 3 0 3 ）。

【 0 1 2 7 】

ヘッダ情報生成部 3 0 0 6 は、コンテンツ位置情報生成部 3 0 0 5 から、c 組の部分コンテンツと特定情報と、暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K とが入力された場合、c 組の部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。続いて、c 組の特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値としてハッシュ値を計算する。そして、特定情報識別子と特定情報を抽出し、c 組の特定情報識別子と特定情報とからなるコンテンツ位置情報 P O S を生成する。さらに、c 組の特定情報識別子とハッシュ値とからなるヘッダ情報 H E A D を生成する。そして、コンテンツ位置情報 P O S とヘッダ情報 H E A D と暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K とを認証情報生成部 3 0 0 8 へ出力する（ステップ S 3 0 4 ）。

【 0 1 2 8 】

認証情報生成部 3 0 0 8 は、ヘッダ情報生成部 3 0 0 6 からコンテンツ位置情報 P O S とヘッダ情報 H E A D と暗号化鍵束 K B とコンテンツ C N T とコンテンツ鍵 C K とが入力された場合、認証情報生成情報格納部 3 0 0 7 にアクセスして、認証情報生成情報 G E N A U T H を取得する。そして、ヘッダ情報 H E A D と認証情報生成情報 G E N A U T H とを用いて、ヘッダ情報 H E A D に対する認証情報である認証情報 A U T H を生成する。そして、コンテンツ位置情報 P O S とヘッダ情報 H E A D と暗号化鍵束 K B と認証情報 A U T H とコンテンツ C N T とコンテンツ鍵 C K とを暗号化部 3 0 0 9 へ出力する（ステップ

S 3 0 5)。

【0129】

暗号化部3009は、認証情報生成部3008からコンテンツ位置情報POSとヘッダ情報HEADと暗号化鍵束KBと認証情報AUTHとコンテンツCNTとコンテンツ鍵CKとが入力される。そして、コンテンツ鍵CKを基に、コンテンツCNTを暗号化し、暗号化コンテンツENCCNTを生成する。そして、暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとを配布部3010へ出力する(ステップS306)。

【0130】

配布部3010は、暗号化部3009から入力された暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとを可搬媒体31へ記録する(ステップS307)。

以上が、不正コンテンツ検知システム3の構成要素である配布センタ30の構成と動作である。続いて、可搬媒体31の構成について説明を行う。

【0131】

＜可搬媒体31の構成＞

可搬媒体31は、例えば、DVD-ROMやCD-ROM等のような可搬媒体であり、図29に示すように、暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとが配布センタ30によって記録されているものとする。

【0132】

以上が、不正コンテンツ検知システム3の構成要素である可搬媒体31の構成である。続いて、実行装置32の構成と動作について説明を行う。

＜実行装置32の構成＞

実行装置32は、図30に示すように、取得部321、デバイス鍵格納部322、コンテンツ鍵取得部323、検証情報格納部324、認証情報検証部325、特定情報選択部326、部分復号化部327、ヘッダ情報検証部328、実行部329とから構成される。

【0133】

(1) 取得部321

取得部321は、可搬媒体31に記録されているデータの読み取りを行い、暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとを取得する。そして、取得した暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとをコンテンツ鍵取得部323へ出力する。

【0134】

(2) デバイス鍵格納部322

デバイス鍵格納部322は、配布センタ30の実行装置情報格納部3003の中の鍵情報の一部を保持するものであり、デバイス鍵格納部322に与えられる鍵情報と暗号化鍵束KBを用いて、コンテンツ鍵CKが取得出来るものである。例えば、実行装置情報格納部3003が図22のような場合、デバイス鍵格納部322には、装置識別子AID_iとデバイス鍵K_i(_iは1からnのいずれか)が与えられる。

【0135】

(3) コンテンツ鍵取得部323

コンテンツ鍵取得部323は、取得部321から暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCCNTとが入力された場合、デバイス鍵格納部322に格納されている鍵情報及び暗号化鍵束KBを用いて、コンテンツ鍵CKを取得する。例えば、暗号化鍵束KBが図22のような場合で、デバイス鍵格納部322には装置識別子AID_iとデバイス鍵DK_i(_iは1からnのいずれか)が与えられている場合、コンテンツ鍵取得部323はデバイス鍵格納部322か

ら装置識別子A I D i とデバイス鍵D K i を取得し、暗号化鍵束K B の中から装置識別子A I D i に対応する暗号化コンテンツ鍵E N C C K i (E N C C K 1 からE N C C K n の何れか) を取得する。そしてデバイス鍵D K i を基に、暗号化コンテンツ鍵E N C C K i を復号化することによって、コンテンツ鍵C K = D e c (D K i 、E N C C K i) を取得する。なお、D e c (K 、C) を暗号文C を復号化鍵K を用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵C K とヘッダ情報H E A D とコンテンツ位置情報P O S と認証情報A U T H と暗号化コンテンツE N C C N T を認証情報検証部3 2 5 へ出力する。

【0 1 3 6】

(4) 検証情報格納部3 2 4

検証情報格納部3 2 4 は、ヘッダ情報H E A D に対する認証情報である認証情報A U T H の正当性を検証するために必要な検証情報V E R を保持するものである。この検証情報V E R に対応する認証情報生成情報G E N A U T H は、配布センタ3 0 の認証情報生成情報格納部3 0 0 7 に格納されている。例えば、検証情報V E R はデジタル署名アルゴリズムの署名検証鍵(公開鍵)である。

【0 1 3 7】

(5) 認証情報検証部3 2 5

認証情報検証部3 2 5 は、コンテンツ鍵取得部3 2 3 からコンテンツ鍵C K とヘッダ情報H E A D とコンテンツ位置情報P O S と認証情報A U T H と暗号化コンテンツE N C C N T とが入力された場合、検証情報格納部3 2 5 に格納されている検証情報V E R を使って、認証情報A U T H が発行センタ3 0 によるヘッダ情報H E A D の正規の認証情報であるかを検証する。例えば、デジタル署名検証アルゴリズムを用いて、認証情報A U T H がヘッダ情報H E A D の正しいデジタル署名であるかを検証するなどである。このデジタル署名検証アルゴリズムは、配布センタ3 0 の認証情報生成部3 0 0 8 で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献1に記載のD S A 方式などである。認証情報検証部3 2 5 は、認証情報A U T H が発行センタ3 0 によるヘッダ情報H E A D の正しい認証情報である場合にのみ、コンテンツ鍵C K とヘッダ情報H E A D とコンテンツ位置情報P O S と暗号化コンテンツE N C C N T を特定情報選択部3 2 6 へ出力する。

【0 1 3 8】

(6) 特定情報選択部3 2 6

特定情報選択部3 2 6 は、認証情報検証部3 2 5 からコンテンツ鍵C K とヘッダ情報H E A D とコンテンツ位置情報P O S と認証情報A U T H と暗号化コンテンツE N C C N T とが入力された場合、ヘッダ情報H E A D に含むc 個の特定情報識別子(P O S I D 1 、
・ ・ ・ 、P O S I D c) の中から、b 個の特定情報識別子(b は1 以上c - 1 以下の自然数) を選択する。ここでは、第三者によってどの特定情報識別子を選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、特定情報選択部3 2 6 が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献2 が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、特定情報選択部3 2 6 が温度センサや湿度センサを有することにより実現出来る。その後、選択されたb 個の特定情報識別子と対応するb 個のハッシュ値から成る被選択ヘッダ情報S E L H E A D を生成する。例として、図3 1 は、特定情報識別子A D D R I D 2 とハッシュ値H A S H 2 、特定情報識別子A D D R I D a とハッシュ値H A S H a を選択した場合の被選択ヘッダ情報S E L H E A D について表している。また、選択されたb 個の特定情報識別子と対応するb 個の特定情報から成る被選択コンテンツ位置情報S E L P O S を生成する。例として、図3 2 は、特定情報識別子A D D R I D 2 と特定情報A D D R 2 、特定情報識別子A D D R I D a と特定情報A D D R a を選択した場合の被選択コンテンツ位置情報S E

L P O Sについて表している。そして、コンテンツ鍵C Kと被選択ヘッダ情報S E L H E A Dと被選択コンテンツ位置情報S E L P O Sと認証情報A U T Hと暗号化コンテンツE N C C N Tとを部分復号化部3 2 7へ出力する。ここで、被選択ヘッダ情報S E L H E A Dにはb組の特定情報識別子と特定情報を、被選択コンテンツ位置情報S E L P O Sにはb組の特定情報識別子とハッシュ値を含むことになる。

【0 1 3 9】

(7) 部分復号化部3 2 7

部分復号化部3 2 7は、特定情報選択部3 2 6からコンテンツ鍵C Kと被選択ヘッダ情報S E L H E A Dと被選択コンテンツ位置情報S E L P O Sと暗号化コンテンツE N C C N Tとが入力された場合、以下の処理を行う。まず、被選択コンテンツ位置情報S E L P O Sの中の一組目の特定情報識別子と特定情報を抽出する。ここでは図3 2の場合を例に挙げて、一組目の特定情報識別子と特定情報をそれぞれA D D R I D 2とA D D R 2とする。そして、暗号化コンテンツE N C C N Tの中から特定情報A D D R 2が特定する暗号化部分コンテンツE N C C N T—2を取得し、コンテンツ鍵C Kを基に復号化を行い、部分コンテンツC N T—2を取得する（例えば、図3 3参照）。続いて、被選択コンテンツ位置情報S E L P O Sの二組目以降の特定情報識別子と特定情報とを同様に抽出し、対応する部分コンテンツを取得する。そして、被選択ヘッダ情報S E L H E A Dと暗号化コンテンツE N C C N Tと、抽出されたb組の特定情報識別子と部分コンテンツと、コンテンツ鍵C Kと、をヘッダ情報検証部3 2 8へ出力する。なお、部分復号化部3 2 7で使用する暗号アルゴリズムは、例えば、非特許文献1に記載のA E S方式などであり、配布センタ3 0の暗号化部3 0 0 9と同じ暗号アルゴリズムを用いる。

【0 1 4 0】

(8) ヘッダ情報検証部3 2 8

ヘッダ情報検証部3 2 8は、部分復号化部3 2 7から被選択ヘッダ情報S E L H E A DとコンテンツC N Tと、b組の特定情報識別子と部分コンテンツと、コンテンツ鍵C Kと、が入力された場合、まず、一組目の特定情報識別子と部分コンテンツに対して、以下の処理を行う。ここでも図3 2の場合を例に挙げて、一組目の特定情報識別子と部分コンテンツをそれぞれA D D R I D 2とC N T—2とする。最初に、部分コンテンツC N T—2に対して、そのハッシュ値Xを計算する。部分コンテンツのハッシュ値を求める方法としては、例えば、一方向性関数を用いる方法があり、非特許文献1に記載のS H A—1アルゴリズムやブロック暗号を用いたC B C—M A Cなどがあり、配布センタ3 0のヘッダ情報生成部3 0 0 8で用いる方法と同じものを用いる。そして、被選択ヘッダ情報S E L H E A Dの中の特定情報識別子A D D R I D 2に対応するハッシュ値H A S H 2と計算されたハッシュ値Xが等しいかどうか確認する。もし、同じ値であれば、二組目以降の特定情報識別子と部分コンテンツに対しても、同様にしてハッシュ値を計算し、被選択ヘッダ情報S E L H E A Dの中の対応する特定情報識別子のハッシュ値と比較する。ここで、b個のハッシュ値が全て等しかった場合にのみ、ヘッダ情報検証部3 2 8は実行部3 2 9へ暗号化コンテンツE N C C N Tとコンテンツ鍵C Kと、を出力する。

【0 1 4 1】

(9) 実行部3 2 9

実行部3 2 9は、ヘッダ情報検証部3 2 8から入力された暗号化コンテンツE N C C N Tに含まれるc個の暗号化部分コンテンツE N C C N T—1、・・・、E N C C N T—cを、コンテンツ鍵C Kを基に逐次復号化を行って部分コンテンツC N T—1、・・・、C N T—cを取得し、逐次その部分コンテンツを実行するものである。例えば、実行部3 2 9はM P E G 2データやM P 3データをデコードする機能を有するデコーダを有していて、M P E G 2形式の動画コンテンツやM P 3形式の音声コンテンツであるコンテンツC N Tを逐次デコードして、外部に出力するようにしても良い。また例えば、実行部3 2 9は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生しても良いし、別の可搬媒体や記録媒体にコンテンツデータを出力しても良いし、コンテンツデータを紙などに印刷してもよい。なお、復号化を行う単位やデコードを行う単位は、コンテン

ツ位置情報生成部3005でコンテンツCNTを分割した単位に限るものではなく、例えば16バイト毎であっても良い。

【0142】

＜実行装置32の動作＞

以上で、実行装置32の構成について説明を行ったが、ここで実行装置32の動作について、図34に示すフローチャートを用いて説明する。なお、実行装置32の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【0143】

取得部321は、可搬媒体31に記録されているデータの読み取りを行い、暗号化鍵束KBとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとをコンテンツ鍵取得部323へ出力する。そして、コンテンツ鍵取得部323は、入力された暗号化鍵束KB及びデバイス鍵格納部322が保持している鍵情報を用いて、コンテンツ鍵CKを取得する。そして、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとを認証情報検証部325へ出力する（ステップS321）。

【0144】

認証情報検証部325は、コンテンツ鍵取得部323からコンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTを入力された場合、検証情報格納部324に格納されている検証情報VERを用いて、認証情報AUTHがヘッダ情報HEADに対する正しい認証情報であるかを検証する（ステップS322）。

【0145】

認証情報検証部325は、認証情報AUTHがヘッダ情報HEADに対する発行センタ30の正しい認証情報である場合にのみ、コンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTとを特定情報選択部326へ出力し、ステップS324へ進む。もし、認証情報AUTHがヘッダ情報HEADに対する正しい認証情報ではない場合、処理を終了する（ステップS323）。

【0146】

特定情報選択部326は、認証情報検証部325からコンテンツ鍵CKとヘッダ情報HEADとコンテンツ位置情報POSと認証情報AUTHと暗号化コンテンツENCNTとを入力された場合、コンテンツ位置情報POSに含まれるc個の特定情報識別子からb個の特定情報識別子を選択する。そして、ヘッダ情報HEADから選択されたb個の特定情報識別子と対応するb個のハッシュ値からなる被選択ヘッダ情報SELHEADを生成する。また、コンテンツ位置情報POSから選択されたb個の特定情報識別子と対応するb個の特定情報からなる被選択コンテンツ位置情報SELPoSを生成する。そして、コンテンツ鍵CKと被選択ヘッダ情報SELHEADと被選択コンテンツ位置情報SELPoSと認証情報AUTHと暗号化コンテンツENCNTとを部分復号化部327へ出力する（ステップS324）。

【0147】

部分復号化部327は、特定情報選択部326からコンテンツ鍵CKと被選択ヘッダ情報SELHEADと被選択コンテンツ位置情報SELPoSと暗号化コンテンツENCNTとを入力される。そして、コンテンツ鍵CKを基に、暗号化コンテンツENCNTに含まれるb個の特定情報のそれぞれに対する暗号化部分コンテンツをそれぞれ復号化し、b個の部分コンテンツを抽出する。そして、被選択ヘッダ情報SELHEADと暗号化コンテンツENCNTと、b組の特定情報識別子と部分コンテンツと、コンテンツ鍵CKと、をヘッダ情報検証部328へ出力する（ステップS325）。

【0148】

ヘッダ情報検証部328は、部分復号化部327から被選択ヘッダ情報SELHEADと暗号化コンテンツENCNTと、b組の特定情報識別子と部分コンテンツと、コンテ

ンツ鍵C Kと、を入力される。そして、各組の部分コンテンツに対して、そのハッシュ値を計算する（ステップS 3 2 6）。

ヘッダ情報検証部3 2 8は、計算したハッシュ値が、被選択ヘッダ情報S E L H E A Dの中の特定情報識別子に対応するハッシュ値と等しいかどうか確認し、もし、全てのハッシュ値が同じ値であれば、ヘッダ情報検証部3 2 8は実行部3 2 9へ暗号化コンテンツE N C C N Tとコンテンツ鍵C Kを出力し、ステップS 3 2 8へ進む。もし、一つでもハッシュ値が一致しなければ、処理を終了する（ステップS 3 2 7）。

【0 1 4 9】

実行部3 2 9は、ヘッダ情報検証部3 2 8から受け取った暗号化コンテンツE N C C N Tの中の暗号化部分コンテンツを、コンテンツ鍵を用いて逐次復号化し、その部分コンテンツを実行する（ステップS 3 2 8）。

以上が、不正コンテンツ検知システム3の構成要素である実行装置3 2の構成と動作である。尚、コンテンツ鍵取得部3 2 3、認証情報検証部3 2 5、特定情報選択部3 2 6等の各機能ブロックは典型的には集積回路であるL S Iとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0 1 5 0】

ここでは、L S Iとしたが、集積度の違いにより、I C、システムL S I、スーパーL S I、ウルトラL S Iと呼称されることもある。

また、集積回路化の手法はL S Iに限るものではなく、専用回路又は汎用プロセサで実現してもよい。L S I製造後に、プログラムすることが可能なF P G A（F i e l d P r o g r a m m a b l e G a t e A r r a y）や、L S I内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用して良い。

【0 1 5 1】

さらには、半導体技術の進歩又は派生する別技術によりL S Iに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム3の効果＞

以上、不正コンテンツ検知システム3について実施の形態に基づいて説明したが、この不正コンテンツ検知システム3においては、配布センタ3 0が、暗号化されたコンテンツC N Tとともに、コンテンツC N Tに対応するヘッダ情報H E A D、及び、ヘッダ情報に対する認証情報A U T H（例えばデジタル署名）、及び、コンテンツ位置情報P O Sを可搬媒体3 1に記録するようにした。そして、実行装置3 2が、コンテンツC N Tの実行、再生開始前に、認証情報A U T Hがヘッダ情報H E A Dに対する正規の認証情報（例えばデジタル署名）であるか検証するとともに、ヘッダ情報H E A Dに含まれるc個のハッシュ値のうち、b個のハッシュ値に絞って検証するようにした。これは、コンテンツC N Tを実行、再生開始する毎に、異なるハッシュ値を選択するようにして、不正者は、どのハッシュ値が選択されるか予想出来ないように注意する。そして、選択されたb個のハッシュ値が共に正当であると検証された場合にのみ、コンテンツC N Tの実行、再生を開始するようにした。そうすることにより、実行装置3 2は、不正な認証情報A U T Hもしくはヘッダ情報H E A DもしくはコンテンツC N Tが記録された可搬媒体3 1のコンテンツC N Tは実行開始しないようになる。これにより、コンテンツC N Tの中のある部分コンテンツを不正な部分コンテンツに差し替えようとしても、その不正な部分コンテンツに差し替えられた部分に対応するハッシュ値の検証が行われた場合、そのコンテンツは実行出来なくなる。つまり、コンテンツC N Tの一部でも不正な部分コンテンツに差し替えた場合、ある確率でコンテンツC N Tを実行できなくなることになる。これは、コンテンツC N Tの中の一部を、不正なコンテンツに差し替えられるような攻撃を防ぐ抑止力となる。

【0 1 5 2】

また、実行装置3 2は、認証情報A U T Hの正当性の検証を、コンテンツC N Tを実行

、再生開始する前に全て行うため、コンテンツC N Tの実行、再生中の特別な処理が必要なくなり、コンテンツC N Tの実行中の処理負荷が軽減されるという効果を有する。

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0153】

(1) 実施の形態1において、認証情報A U T Hは、ヘッダ情報H E A Dに対するデジタル署名であったが、実行装置12においてヘッダ情報H E A Dの正当性を検証出来るものであれば、どのようなものでも良い。例えば、デジタル署名方式を用いずにA E Sなどの秘密鍵暗号を用いても同様のことが実現出来る。まず、認証情報生成情報格納部1007及び検証情報格納部125には、同じ鍵Kが与えられているとする。そして、認証情報生成部1008では、鍵Kを用いてヘッダ情報H E A Dを暗号化した暗号文を認証情報A U T Hとする。認証情報検証部126では、鍵Kを用いて入力された認証情報A U T Hを復号化し、その復号結果がヘッダ情報H E A Dと一致していれば、認証情報A U T Hは正当であると判断する。このようにして、デジタル署名アルゴリズムを使用しなくても、ヘッダ情報の正当性を検証することが出来る。同様に、一方向性関数や鍵付き一方向性関数などを用いても同様に実現出来る。なお、実施の形態2及び実施の形態3においても、同様にデジタル署名アルゴリズムの代わりに、A E Sなどの秘密鍵暗号や一方向性関数や鍵付き一方向性関数などを利用出来る。

【0154】

(2) 実施の形態1の可搬媒体11では、暗号化コンテンツ位置情報E N C P O Sが記録されていたが、図35のように、可搬媒体11には、暗号化していないコンテンツ位置情報P O Sをそのまま記録するようにしても良い。こうすることにより、実行装置12で暗号化コンテンツ位置情報E N C P O Sを復号化する必要がなくなる。なお、実施の形態2においても、同様のことが実現出来る。

【0155】

(3) 実施の形態1の可搬媒体11に記録される認証情報A U T Hは、ヘッダ情報H E A Dに対する配布センタ10のデジタル署名であったが、k個(kは1以上の自然数)の代表部分コンテンツP 1—C N T、・・・、P k—C N Tを連結した値に対する配布センタ10のデジタル署名であっても良い。

これは、可搬媒体11には、図36で示すように、ヘッダ情報H E A Dと認証情報A U T Hの代わりに、コンテンツ認証情報C N T A U T Hを記録するようにし、コンテンツ認証情報C N T A U T Hが、図37で示すように、特定情報識別子とその特定情報識別子に対応する代表部分コンテンツのデジタル署名のk組から成り、さらに、実行装置12の認証情報検証部126では、ヘッダ情報H E A Dに対する認証情報A U T Hの正当性を検証するのではなく、特定情報識別子に対応する代表部分コンテンツに対するデジタル署名(S 1、・・・、S k)の正当性を検証するようにすることによって、実現出来る。

【0156】

また、別の実現方法としては、コンテンツ認証情報C N T A U T Hは、図37で示すように、各特定情報識別子に対応する代表部分コンテンツのそれぞれのデジタル署名を含んでいなくてもよく、図38で示すように、各特定情報識別子に対応する代表部分コンテンツを連結した一つの値に対するデジタル署名S I Gを一つ含んでいてもよい。

こうすることにより、可搬媒体11にヘッダ情報H E A Dを記録しなくてすむため、記録データのサイズを削減することが出来る。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

【0157】

(4) 実施の形態1の可搬媒体11には、暗号化コンテンツ位置情報E N C P O Sが記録されていたが、図39のように、可搬媒体11には、暗号化コンテンツ位置情報E N C P O Sを記録せずに、実行装置12のコンテンツ位置情報格納部に暗号化コンテンツ位置

情報ENCPOSを保持するようにして、コンテンツ位置情報取得部124は、コンテンツ位置情報格納部にアクセスして、暗号化コンテンツ位置情報ENCPOSを取得するようにしてもよい。

【0158】

また、可搬媒体11にはさらに、図40で示すように、コンテンツ位置情報POSを識別するコンテンツ位置情報識別子CNTAIDi (CNTAID1、・・・、CNTAIDgのいずれか、gは1以上の自然数) が記録されており、実行装置12のコンテンツ位置情報格納部は、コンテンツ位置情報識別子CNTAID1、・・・、CNTAIDgのそれぞれに対応する暗号化コンテンツ位置情報ENCPOS1、・・・、ENCPOSgを保持しており、コンテンツ位置情報取得部124は、コンテンツ位置情報格納部にアクセスして、コンテンツ位置情報識別子CNTAIDiに対応する暗号化コンテンツ位置情報ENCPOSi (ENCPOS1、・・・、ENCPOSgのいずれか) を取得するようにしてもよい。

【0159】

こうすることにより、可搬媒体11に暗号化コンテンツ位置情報ENCPOSを記録する必要がなくなるため、記録データのサイズを削減することが出来る。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

なお、変形例(2)と組み合わせて、実行装置12のコンテンツ位置情報格納部には、暗号化コンテンツ位置情報ENCPOSではなく、暗号化されていないコンテンツ位置情報POSをそのまま格納しても良い。

【0160】

(5) 実施の形態1の認証情報AUTHは、図8のように、k個の特定情報識別子とk個のハッシュ値を連結した値に対する認証情報であったが、これに限るものではない。例えば、k個のハッシュ値を連結した値であっても良い。さらに、図41のように、k個の特定情報識別子とk個のハッシュ値に加え、コンテンツ鍵CKを連結した値に対する認証情報であっても良い。この場合、可搬媒体11に記録するヘッダ情報としては、図8のように、k組の特定情報識別子とハッシュ値のみにする。こうすることにより、コンテンツ鍵CKを持たないものは、認証情報AUTHの正当性すら検証出来なくなり、安全性がより高まる。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

【0161】

(6) 実施の形態1の認証情報AUTHは、図8のように、k個の特定情報識別子とk個のハッシュ値を連結した値に対する認証情報であったが、図42のように、k個の特定情報識別子とk個のハッシュ値に加え、コンテンツCNTのサイズであるコンテンツサイズCNTSIZEを連結した値に対する認証情報であっても良い。こうすることにより、コンテンツCNTのサイズも認証情報AUTHに影響するため、安全性がより高まる。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

【0162】

(7) 実施の形態2の実行装置22の取得部221では、m種類のヘッダ識別子のうち、1種類のヘッダ識別子のみを選択していたが、1種類ではなく、s種類(sは2以上m以下の自然数)のヘッダ識別子を選択し、s種類のヘッダ情報と認証情報の正当性を検証するようにしてもよい。こうすることにより、ヘッダ情報と認証情報の正当性検証を一度にs回行うことが出来、処理時間は多くかかるが、安全性を向上させることが出来る。

【0163】

(8) 実施の形態1の可搬媒体11では、暗号化コンテンツENCNTが記録されていたが、可搬媒体11には、暗号化されていないコンテンツCNTをそのまま記録するようにしても良い。こうすることにより、実行装置12で暗号化コンテンツENCNTを復号化する必要がなくなる。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

【0164】

(9) 実施の形態1の配布センタ10は、図2で示すような構成に限るものではない。

例えば、認証情報AUTHなどを可搬媒体11へ記録する配布部1010と、ヘッダ情報HEADに対する認証情報を生成する認証情報生成部1008とを、別の主体が行うようにしても良い。例えば、コンテンツCNTに対する認証情報を生成するのはコンテンツCNTの正規の著作権者であり、認証情報AUTHなどを可搬媒体11へ記録するのはディスク製造業者であるなど、が考えられる。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

【0165】

(10) 実施の形態1の配布センタ10の認証情報生成情報格納部1007、及び、実行装置12の検証情報格納部125は、これに限るものではない。例えば、以下のような例が考えられる。

(i) 一つの例として、認証情報生成情報格納部1007は、図43で示すように、1つの認証情報生成情報GENAUTH_i (GENAUTH₁、・・・、GENAUTH_wのいずれか wは1以上の自然数) と対応する検証情報識別子VERID_i を保持しており、検証情報格納部125は、図44で示すように、w組の検証情報識別子(GENAUTH₁、・・・、GENAUTH_w) と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報(VER₁、・・・、VER_w) を保持している場合が考えられる。この場合、配布センタ10の配布部1010は、可搬媒体11に、認証情報生成情報格納部1007に格納されている検証情報識別子GENAUTH_i を加えて記録するようにして、さらに、実行装置12の認証情報検証部126は、可搬媒体11に記録されている検証情報識別子GENAUTH_i に対応する検証情報VER_i (VER₁、・・・、VER_wのいずれか) を検証情報格納部125から取得し、その検証情報VER_i を基に、認証情報AUTHを検証することになる。

【0166】

(ii) 別の例として、認証情報生成情報格納部1007には、認証情報生成情報GENAUTHと対応する検証情報VERを保持しており、検証情報格納部125には、何も保持していない場合が考えられる。この場合、配布センタ10の配布部1010は、可搬媒体11に、認証情報生成情報格納部1007に格納されている検証情報VERを加えて記録するようにして、さらに、実行装置12の認証情報検証部126は、可搬媒体11に記録されている検証情報VERを基に、認証情報AUTHを検証することになる。

【0167】

(iii) さらに別の例として、認証情報生成情報格納部1007には、図45で示すように、認証情報生成情報GENAUTHと対応する検証情報VER、及び、第三者機関によって生成された検証情報VERに対する認証情報(例えばセンタによるデジタル署名)であるセンタ認証情報CAUTHを保持しており、検証情報格納部125は、図46で示すように、第三者機関の検証情報であるセンタ検証情報CVER(例えばセンタのデジタル署名の署名検証鍵)を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関(Trusted Third Party)や、鍵配布センタなどである。この場合、配布センタ10の配布部1010は、可搬媒体11に、認証情報生成情報格納部1007に格納されている検証情報VER及びセンタ認証情報CAUTHを加えて記録するようにして、さらに、実行装置12の認証情報検証部126は、検証情報格納部125のセンタ検証情報CVERを用いて、可搬媒体11に記録されているセンタ認証情報CAUTHが、検証情報VERに対する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報VERを基に、認証情報AUTHを検証するようにすることになる。

【0168】

このようにすることによって、配布センタ10が複数存在している場合にそれぞれの配布センタ10に別の検証情報を設定したとしても、実行装置12に予め各検証情報を保持しておく必要がなくなる。なお、実施の形態2及び実施の形態3においても、同様のことが実現出来る。

(11) 変形例(10)において、実行装置12は、さらに、無効検証情報を外部から

受信するようにしてもよい。例えば、変形例 11 の (i) の場合、無効検証情報には、検証情報識別子が含まれており、実行装置 1 2 には、外部から無効検証情報として検証情報識別子 G E N A U T H j を受信した場合に、検証情報格納部 1 2 5 に格納されている検証情報識別子 G E N A U T H j に対応する検証情報 V E R j を無効化する検証情報無効化部を備えていてもよい。

【 0 1 6 9 】

また、変形例 (1 0) の (i i) 及び (i i i) の場合、無効検証情報には、検証情報が含まれており、実行装置 1 2 の検証情報格納部 1 2 5 は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部 1 2 6 は、検証情報格納部 1 2 5 の無効検証情報に、可搬媒体 1 1 に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツの実行開始を行わないようにしてもよい。

【 0 1 7 0 】

なお、実行装置 1 2 が外部から無効検証情報を受信する方法としては、可搬媒体 1 1 や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。このようにすることによって、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。なお、実施の形態 2 及び実施の形態 3 においても、同様のことが実現出来る。

【 0 1 7 1 】

(1 2) 変形例 (1 1) において、実行装置 1 2 は、最新の無効検証情報のみを検証情報格納部 1 2 5 に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置 1 2 は、検証情報格納部 1 2 5 が保持する無効検証情報よりも発行日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部 1 2 5 に上書きするようにしてもよいし、また、無効検証情報には発行 I D が記載されており、実行装置 1 2 は、検証情報格納部 1 2 5 が保持する無効検証情報よりも発行 I D が最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部 1 2 5 に上書きするようにしてもよい。なお、実施の形態 2 及び実施の形態 3 においても、同様のことが実現出来る。

【 0 1 7 2 】

(1 3) 実施の形態 1 のコンテンツ C N T は、動画データや音声データなどのコンテンツであったが、コンピュータプログラムであっても良い。この場合、実行装置 1 2 は、コンピュータプログラムを実行するために必要な C P U やメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置 1 2 では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。なお、実施の形態 2 及び実施の形態 3 においても、同様のことが実現出来る。

【 0 1 7 3 】

(1 4) 実施の形態 1 の配布センタ 1 0 では、コンテンツ位置情報生成部 1 0 0 5 においてコンテンツ C N T に対するコンテンツ位置情報 P O S を生成していたが、配布センタ 1 0 が一以上のコンテンツ位置情報 P O S を保持するコンテンツ位置情報格納部を有していて、コンテンツ位置情報生成部 1 0 0 5 はコンテンツ位置情報格納部からいずれかのコンテンツ位置情報 P O S を取得するようにしても良い。こうすることにより、コンテンツ位置情報 P O S を予めまとめて作成しておくことが出来る。なお、実施の形態 2 及び実施の形態 3 においても、同様のことが実現出来る。

【 0 1 7 4 】

(1 5) 実施の形態 1 の配布センタ 1 0 では、コンテンツ鍵生成部 1 0 0 2 においてコンテンツ鍵 C K を生成していたが、配布センタ 1 0 が一以上のコンテンツ鍵 C K を保持するコンテンツ鍵格納部を有していて、コンテンツ鍵生成部 1 0 0 2 はコンテンツ鍵格納部からいずれかのコンテンツ鍵 C K を取得するようにしても良い。こうすることにより、コンテンツ鍵 C K を予めまとめて作成しておくことが出来る。なお、実施の形態 2 及び実施

の形態３においても、同様のことが実現出来る。

【０１７５】

（１６）実施の形態１の実行装置１２のコンテンツ鍵取得部１２３では、暗号化鍵束ＫＢ、及びデバイス鍵格納部１２２に格納されている情報を用いて、コンテンツ鍵ＣＫを取得していたが、配布センタ１０がデバイス鍵格納部１２２の替わりに、コンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部１２３はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ１０は可搬媒体１１に暗号化鍵束ＫＢを記録する必要はなく、実行装置１２は暗号化鍵束ＫＢを受信する必要もない。こうすることにより、可搬媒体１１に暗号化鍵束ＫＢを記録しなくすむため、記録データのサイズを削減することが出来る。なお、実施の形態２及び実施の形態３においても、同様のことが実現出来る。

【０１７６】

（１７）実施の形態１において、配布センタ１０は、可搬媒体１１を介して実行装置１２へコンテンツＣＮＴに関する情報を配布していたが、これに限るものではない。例えば、配布センタ１０と実行装置１２がインターネット等の通信ネットワークに接続されており、配布センタ１０は、その通信ネットワークを介して実行装置１２へコンテンツＣＮＴに関する情報を配布してもよいし、他にも通信ネットワークが放送網であってもよい。なお、実施の形態２及び実施の形態３においても、同様のことが実現出来る。

【０１７７】

（１８）実施の形態３において、実行装置３２は可搬媒体３１内のコンテンツＣＮＴを実行開始する前に、そのコンテンツＣＮＴが不正なものであるか検証していたが、これに限るものではない。例えば、可搬媒体３１が光ディスクであり、実行装置３２がディスクトレイを有している場合、可搬媒体３１が実行装置３２のディスクトレイに挿入された場合に、そのコンテンツＣＮＴが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体３１内のコンテンツＣＮＴをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時１度しか検証しないですむようになるため、コンテンツＣＮＴの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体３１がＳＤカード等の外部メモリで、実行装置３２が外部メモリスロットを有している場合にも、同様のことが実現出来る。また、実施の形態１及び２においても、同様のことが実現出来る。

【０１７８】

（１９）実施の形態３において、配布センタ３０は、可搬媒体３１にヘッダ情報ＨＥＡＤを記録するようにしていたが、可搬媒体３１にヘッダ情報ＨＥＡＤを記録しないようにしても良い。これは、例えば、実行装置３２は、選択された部分コンテンツから計算されるハッシュ値が、ヘッダ情報ＨＥＡＤに含まれるハッシュ値と一致しているか検証する代わりに、図４７で示すように、部分コンテンツを基にハッシュ値を生成し、それらハッシュ値からヘッダ情報ＨＥＡＤを生成し、可搬媒体３１に記録されている認証情報ＡＵＴＨが生成したヘッダ情報ＨＥＡＤに対する正規の認証情報（例えばデジタル署名）であるか検証することで実現できる。こうすることにより、可搬媒体３１に記録するデータサイズを小さくすることが出来る。なお、実施の形態１及び２においても、同様のことが実現出来る。

【０１７９】

（２０）実施の形態３において、実行装置３２は、選択された部分コンテンツから計算されるハッシュ値が、ヘッダ情報ＨＥＡＤに含まれるハッシュ値と一致しているか検証していたが、これに限るものではない。例えば、図４８で示すように、実行装置３２は、選択された部分コンテンツからハッシュ値を計算し、その計算したハッシュ値を可搬媒体３１に記録されているヘッダ情報ＨＥＡＤの対応するハッシュ値と入れ替え、図４９で示すように、第二ヘッダ情報ＨＥＡＤｘを生成する。そして、可搬媒体３１に記録されている認証情報ＡＵＴＨが第二ヘッダ情報ＨＥＡＤｘの正規の認証情報（例えばデジタル署名）であるか検証するようにしてもよい。こうすることにより、実行装置３２において、ハッ

シュ値が一致しているか検証する必要がなくなり、計算量の削減が実現出来る。なお、実施の形態1及び2においても、同様のことが実現出来る。

【0180】

(21) 実施の形態3のコンテンツ位置情報生成部3005において、図50のように、外部から要求情報REQを受信するようにして、その要求情報REQを基にコンテンツCNTを分割するようにしても良い。この要求情報REQは、コンテンツCNTを区切るための情報であり、例えば、64キロバイト単位、1メガバイト単位、1秒単位、1分単位、1秒単位といった情報である。これは、例えば、コンテンツ位置情報生成部3005がキーボードやマウスと接続されていることにより実現できる。さらに、それぞれの部分コンテンツのサイズ(分割単位)は、全て同じである必要はない、それぞれ異なっても良い。また、コンテンツを分割する数(c)は、コンテンツCNTに応じて変えても良い。

【0181】

また、コンテンツを分割する単位は、システム共通のパラメータとして与えられていても良い。この場合、可搬媒体31にはコンテンツ位置情報POSを格納しておく必要はない。

(22) 実施の形態3において、可搬媒体31にはヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTとをそれぞれ一つずつ格納していたが、これに限るものではない。例えば、図51で示すように、可搬媒体31にはヘッダ情報HEADとコンテンツ位置情報POSと暗号化コンテンツENCNTをそれぞれz個(zは2以上の自然数)格納しても良い。このような場合、以下のようなことが実現出来る。ここでは、例えば、可搬媒体31が光ディスクであり、実行装置32はディスクトレイを有しているとする。この場合、可搬媒体31が実行装置32のディスクトレイに挿入された時に、複数のコンテンツを構成する全ての部分コンテンツの中からr個の部分コンテンツを選択しそのハッシュ値を計算し、そのr個(rは1以上の自然数)のハッシュ値がヘッダ情報の中のハッシュ値と一致しているかどうかを行うようにする。そして、複数あるコンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツを構成する部分コンテンツの中からd個(dは1以上r-1以下の自然数)の部分コンテンツを選択しそのハッシュ値を計算し、ヘッダ情報に含まれるハッシュ値と一致しているか検証を行うようにしても良い。つまり、可搬媒体31が実行装置32のディスクトレイに挿入された場合に一度のみ、ある程度の数のハッシュ値の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数のハッシュ値を検証するようにする。これにより、ディスクトレイに挿入された可搬媒体31内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体31は光ディスク出なくてもよく、例えばSDカード等の外部メモリであっても同様のことが実現出来る。また、実施の形態1及び2においても、同様のことが実現出来る。

【0182】

(23) 実施の形態3において、各ハッシュ値(HASH1、・・・、HASHc)は、部分コンテンツに対する属性値(ハッシュ値)であったが、これに限るものではない。例えば、部分コンテンツと特定情報(例えば物理アドレスなど)を連結した値に対する属性値(ハッシュ値)であってもよい。これにより、コンテンツCNTの中のある部分コンテンツを不正な部分コンテンツに差し替えようとする攻撃に対する安全性をより向上させることが出来る。なお、実施の形態1及び実施の形態2においても、同様のことが実現出来る。

【0183】

(24) 実施の形態3においては、実行装置32の認証情報検証部325及びヘッダ情報検証部328における検証結果の両方、もしくは、いずれかが不正である場合、暗号化コンテンツENCNTの復号化及び実行、再生を禁止するようにしていたが、これに限るものではない。例えば、暗号化コンテンツENCNTの復号化及び実行、再生を禁止

するに加え、実行部 3 2 9 では、実行、再生が禁止されている旨、外部に出力（例えば、ディスプレイに「不正なコンテンツです」と表示する）するようにしても良い。また、暗号化コンテンツ E N C C N T の復号化及び実行、再生を禁止するのではなく、暗号化コンテンツ E N C C N T の復号化及び実行、再生は行うが、同時に外部に警告を出力（例えば、ディスプレイに「警告：不正なコンテンツです」と表示する）するようにしても良い。またさらに、実行装置 3 2 とサーバ（配布センタ 3 2 や別のセンタ）とが通信ネットワーク等で接続されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。またさらに、実行装置 3 2 では以後、あらゆる暗号化コンテンツ E N C C N T の復号化及び実行、再生を禁止するようにしてもよい。なお、実施の形態 1 及び実施の形態 2 においても、同様のことが実現出来る。

【0184】

（25）実施の形態 3 の可搬媒体 3 1 には、コンテンツ位置情報 P O S が記録されていたが、これに限るものではない。例えば、図 5 2 のように、可搬媒体 3 1 には、暗号化されたコンテンツ位置情報 P O S を記録するようにしても良い。ここで用いる鍵は、例えば、コンテンツ鍵 C K などが利用可能である。これにより、鍵を知らない者はコンテンツ位置情報 P O S を取得出来なくなるため、コンテンツ C N T の中のある部分コンテンツを不正な部分コンテンツに差し替えようとする攻撃に対する安全性をより向上させることが出来る。

【0185】

（26）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、C D、M O、D V D、S D メモリカード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0186】

（27）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【0187】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人・団体・会社）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般、特に記録媒体や可搬媒体（例えば光ディスクやメモリカード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【0188】

さらに、コンテンツは、動画データや音声データなどに限らず、コンピュータプログラム等にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しないように出来る。そのため、セキュアな処理環境を実現するコンピュータシステム全般、特に O S

(Operating System) 等としても有用である。

【図面の簡単な説明】

【0189】

【図1】 本発明の実施の形態1における不正コンテンツ検知システムの概要図

【図2】 本発明の実施の形態1における配布センタ10の構成例を示す図

【図3】 本発明の実施の形態1におけるコンテンツCNTの一例を示す図

【図4】 本発明の実施の形態1における実行装置情報格納部1003の構成例を示す図

【図5】 本発明の実施の形態1における暗号化鍵束KBの一例を示す図

【図6】 本発明の実施の形態1における代表部分コンテンツと特定情報の一例を示す図

【図7】 本発明の実施の形態1におけるコンテンツ位置情報POSの一例を示す図

【図8】 本発明の実施の形態1におけるヘッダ情報HEADの一例を示す図

【図9】 本発明の実施の形態1における暗号化コンテンツENC CNTの一例を示す図

【図10】 本発明の実施の形態1における配布センタ10の処理の流れ図（一例）

【図11】 本発明の実施の形態1における可搬媒体11に記録されるデータの一例

【図12】 本発明の実施の形態1における実行装置12の構成例を示す図

【図13】 本発明の実施の形態1における実行装置12の処理の流れ図（一例）

【図14】 本発明の実施の形態2における不正コンテンツ検知システムの概要図

【図15】 本発明の実施の形態2における配布センタ20の構成例を示す図

【図16】 本発明の実施の形態2における配布センタ20の処理の流れ図（一例）

【図17】 本発明の実施の形態2における可搬媒体21に記録されるデータの一例

【図18】 本発明の実施の形態2における実行装置22の構成例を示す図

【図19】 本発明の実施の形態2における実行装置22の処理の流れ図（一例）

【図20】 本発明の実施の形態3における不正コンテンツ検知システムの概要図

【図21】 本発明の実施の形態3における配布センタ30の構成例を示す図

【図22】 本発明の実施の形態3における実行装置情報格納部3003の構成例を示す図

【図23】 本発明の実施の形態3における暗号化鍵束KBの一例を示す図

【図24】 本発明の実施の形態3におけるコンテンツCNTの一例を示す図

【図25】 本発明の実施の形態3におけるコンテンツ位置情報POSの一例を示す図

【図26】 本発明の実施の形態3におけるヘッダ情報HEADの一例を示す図

【図27】 本発明の実施の形態3における暗号化コンテンツENC CNTの一例を示す図

【図28】 本発明の実施の形態3における配布センタ30の処理の流れ図（一例）

【図29】 本発明の実施の形態3における可搬媒体31に記録されるデータの一例

【図30】 本発明の実施の形態3における実行装置32の構成例を示す図

【図31】 本発明の実施の形態3における被選択ヘッダ情報SEL HEADの一例を示す図

【図32】 本発明の実施の形態3における被選択コンテンツ位置情報SEL POSの一例を示す図

【図33】 本発明の実施の形態3における暗号化コンテンツENC CNTの一例を示す図

【図34】 本発明の実施の形態1における実行装置12の処理の流れ図（一例）

【図35】 可搬媒体11に記録されるデータの別の一例

【図36】 可搬媒体11に記録されるコンテンツ認証情報CNT AUTHの一例

【図37】 可搬媒体11に記録されるデータの別の一例

【図38】 可搬媒体11に記録されるコンテンツ認証情報CNT AUTHの別の一例

【図39】 可搬媒体11に記録されるデータの別の一例

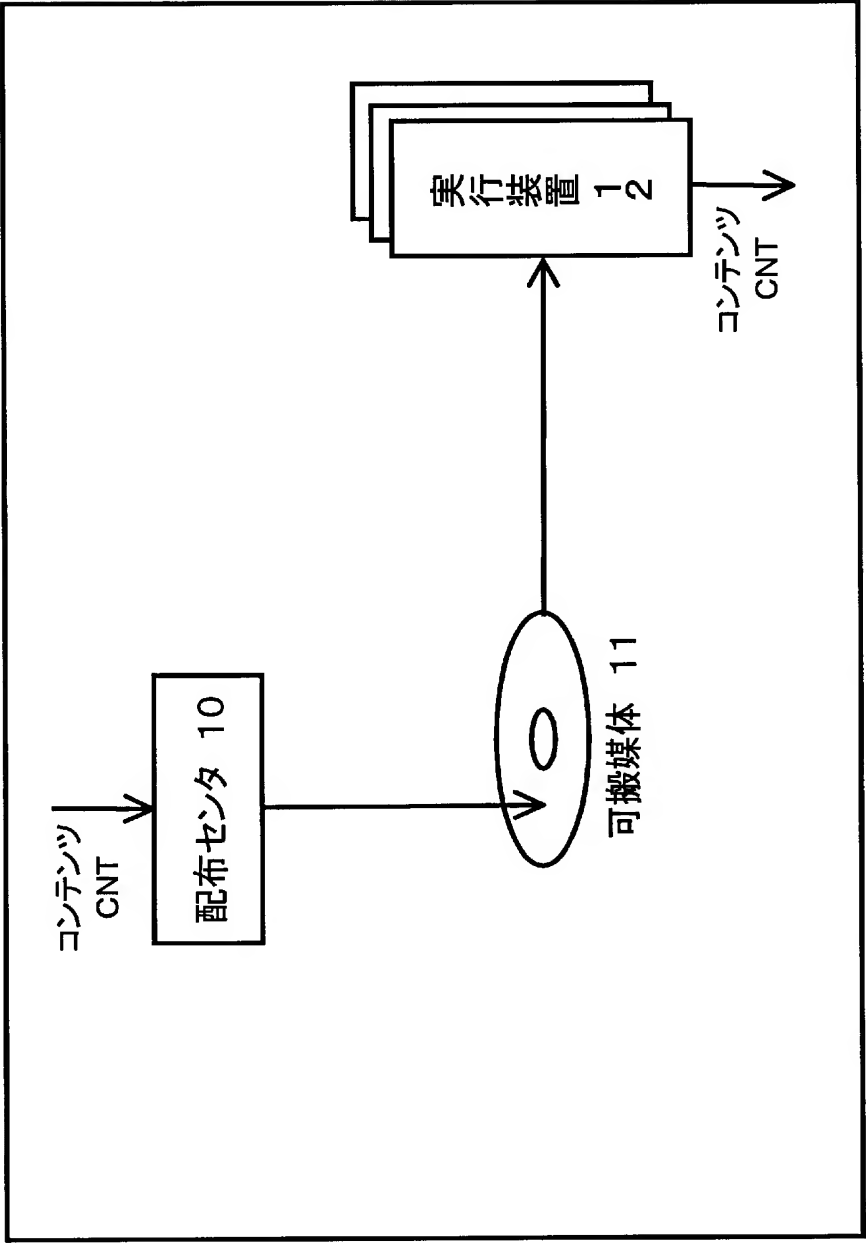
- 【図 4 0】可搬媒体 1 1 に記録されるデータの別の一例
- 【図 4 1】認証情報 A U T H を作成するヘッダ情報 H E A D の別の一例
- 【図 4 2】ヘッダ情報 H E A D の別の一例
- 【図 4 3】認証情報生成情報格納部 1 0 0 7 の別の一例
- 【図 4 4】検証情報格納部 1 2 5 の別の一例
- 【図 4 5】認証情報生成情報格納部 1 0 0 7 の別の一例
- 【図 4 6】検証情報格納部 1 2 5 の別の一例
- 【図 4 7】本発明の実施の形態 3 における可搬媒体 3 1 に記録されるデータの別の一例
- 【図 4 8】本発明の実施の形態 3 における可搬媒体 3 1 に記録されるデータの別の一例
- 【図 4 9】本発明の実施の形態 3 における第二ヘッダ情報 H E A D x の一例
- 【図 5 0】本発明の実施の形態 3 における配布センタ 3 0 の構成例を示す別の図
- 【図 5 1】本発明の実施の形態 3 における可搬媒体 3 1 に記録されるデータの別の一例
- 【図 5 2】本発明の実施の形態 3 における可搬媒体 3 1 に記録されるデータの別の一例
- 【図 5 3】従来技術の可搬媒体に記録されるデータ

【符号の説明】

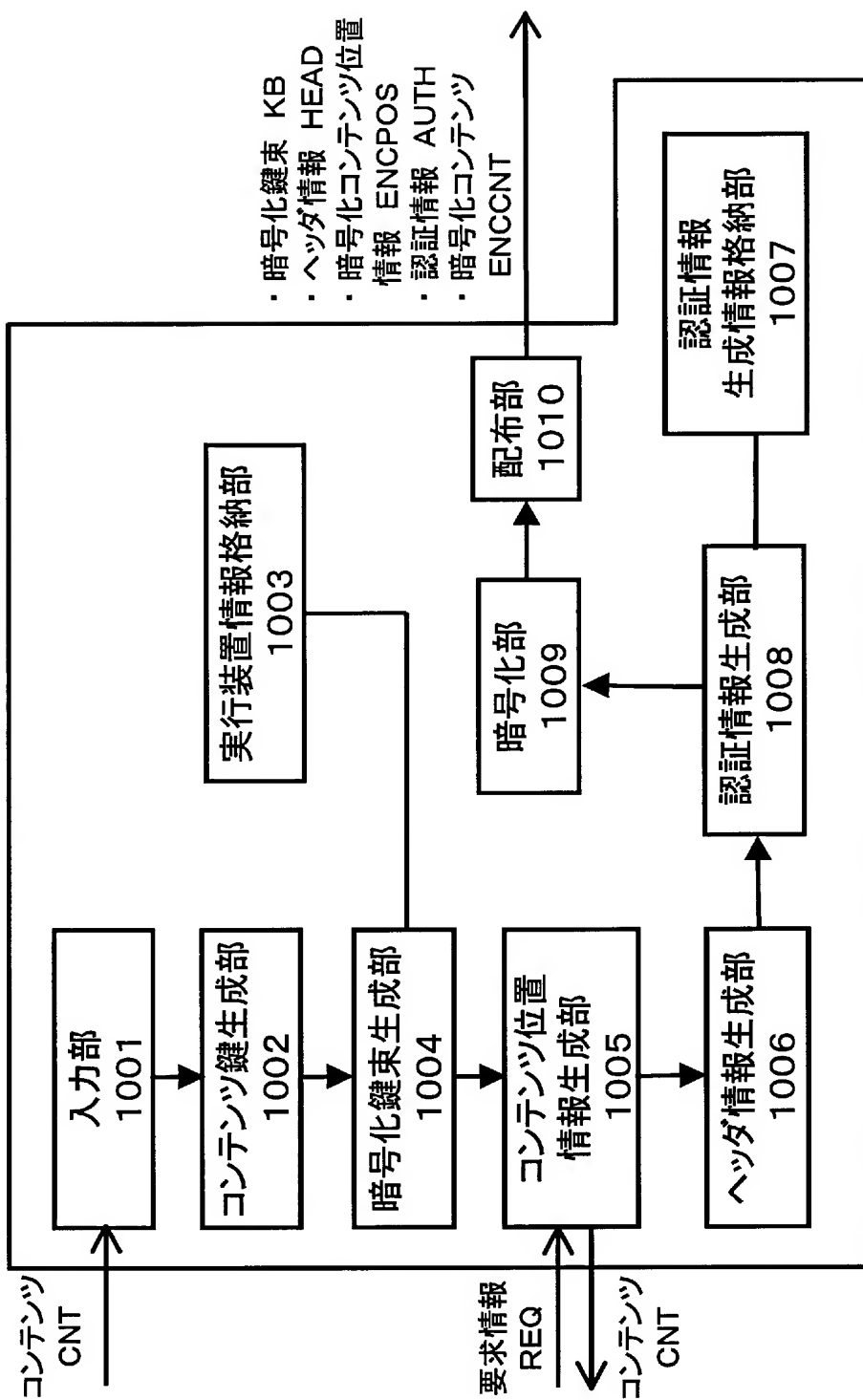
【 0 1 9 0 】

- 1 0、2 0、3 0 配布センタ
- 1 1、2 1、3 1 可搬媒体
- 1 2、2 2、3 2 実行装置
- 1 0 0 1、3 0 0 1 入力部
- 1 0 0 2、3 0 0 2 コンテンツ鍵生成部
- 1 0 0 3、3 0 0 3 実行装置情報格納部
- 1 0 0 4、3 0 0 4 暗号化鍵束生成部
- 1 0 0 5、2 0 0 5、3 0 0 5 コンテンツ位置情報生成部
- 1 0 0 6、2 0 0 6、3 0 0 6 ヘッダ情報生成部
- 1 0 0 7、3 0 0 7 認証情報生成情報格納部
- 1 0 0 8、2 0 0 8、3 0 0 8 認証情報生成部
- 1 0 0 9、2 0 0 9、3 0 0 9 暗号化部
- 1 0 1 0、2 0 1 0、3 0 1 0 配布部
- 1 2 1、2 2 1、3 2 1 取得部
- 1 2 2、3 2 2 デバイス鍵格納部
- 1 2 3、3 2 3 コンテンツ鍵取得部
- 1 2 4 コンテンツ位置情報取得部
- 3 2 6 特定情報選択部
- 1 2 5、3 2 4 検証情報格納部
- 1 2 6、3 2 5 認証情報検証部
- 1 2 7、3 2 7 部分復号化部
- 1 2 8、3 2 8 ヘッダ情報検証部
- 1 2 9、3 2 9 実行部

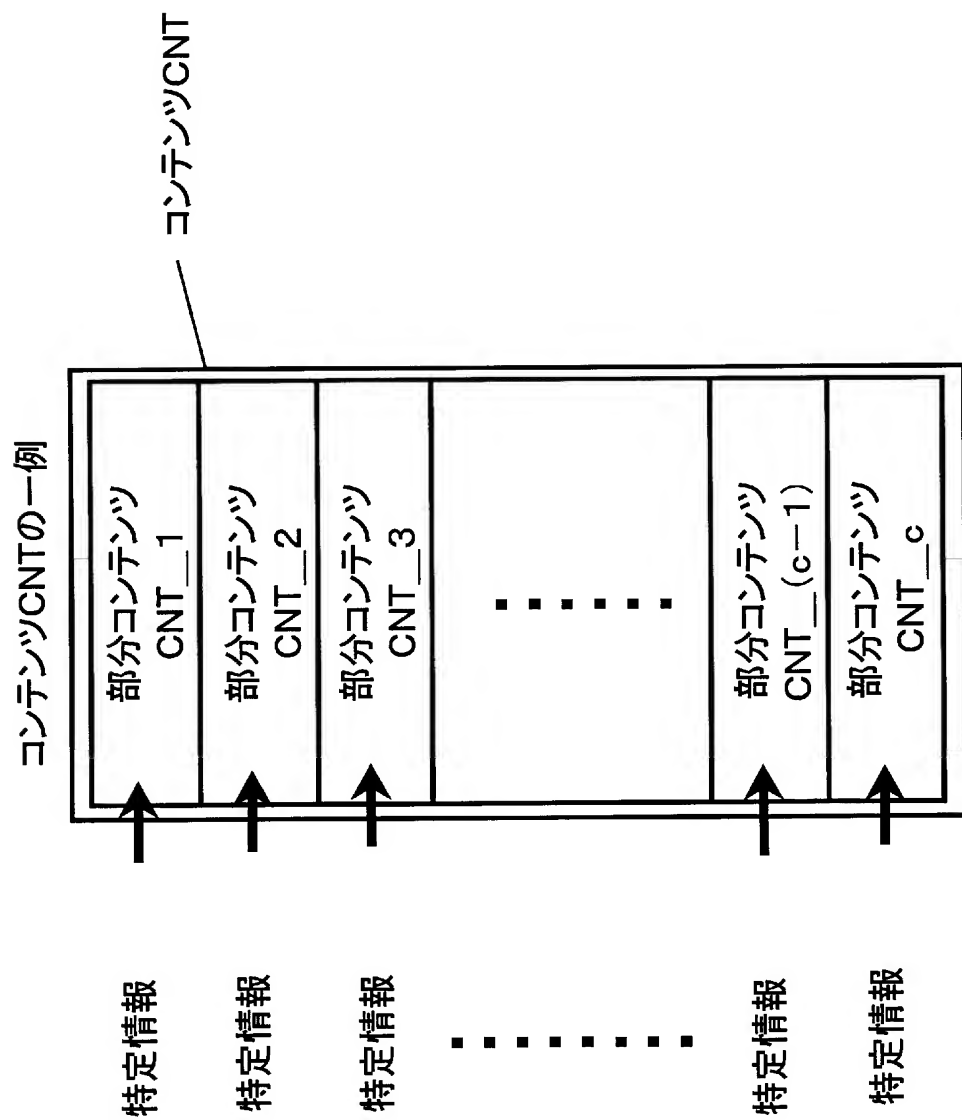
不正コンテンツ検知システム1



配布センタ 10 の一例



- ・ 暗号化鍵束 KB
- ・ ヘッダ情報 HEAD
- ・ 暗号化コンテンツ位置情報 ENCPOS
- ・ 認証情報 AUTH
- ・ 暗号化コンテンツ



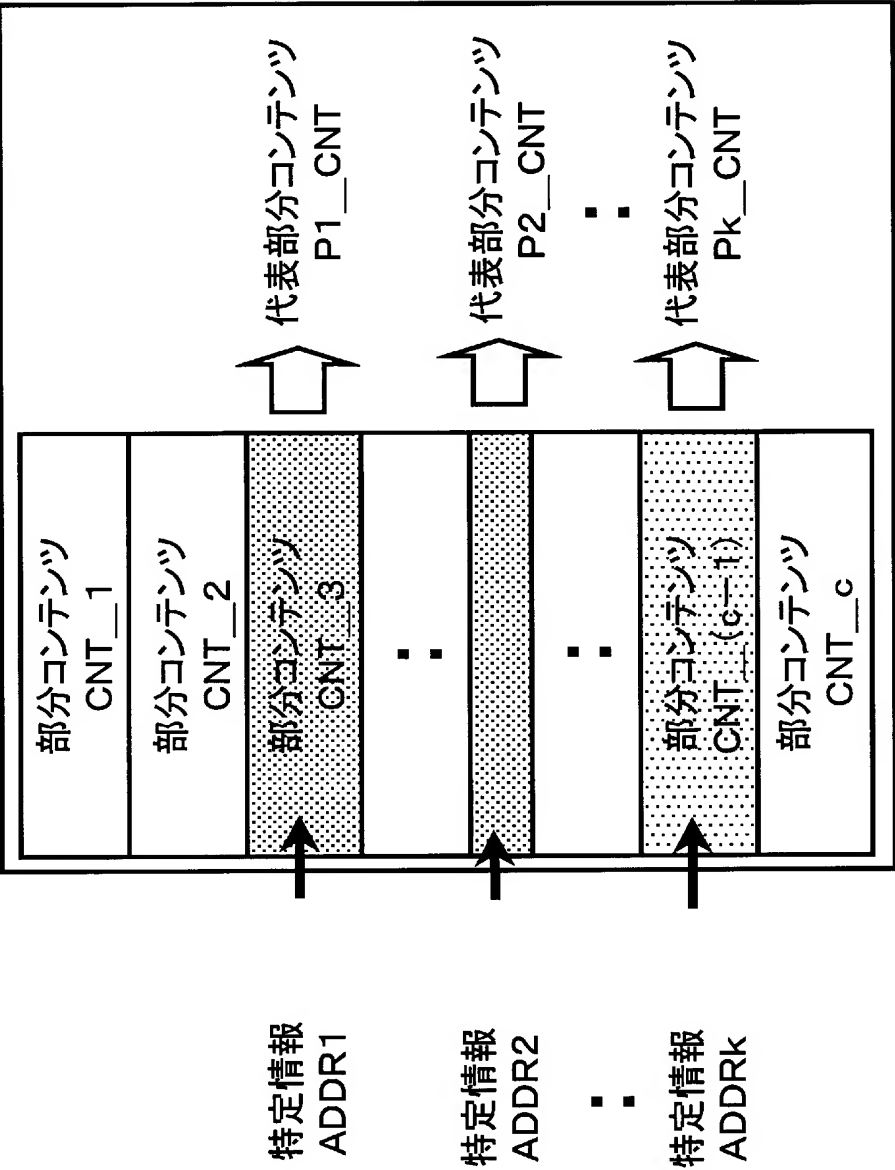
実行装置情報格納部1003の一例

装置識別子 AID1	デバイス鍵 DK1
装置識別子 AID2	デバイス鍵 DK2
装置識別子 AID3	デバイス鍵 DK3
・ ・ ・	・ ・ ・
装置識別子 AIDn	デバイス鍵 DKn

暗号化鍵束 KBの一例



代表部分コンテンツと特定情報の一例
—— コンテンツCNT

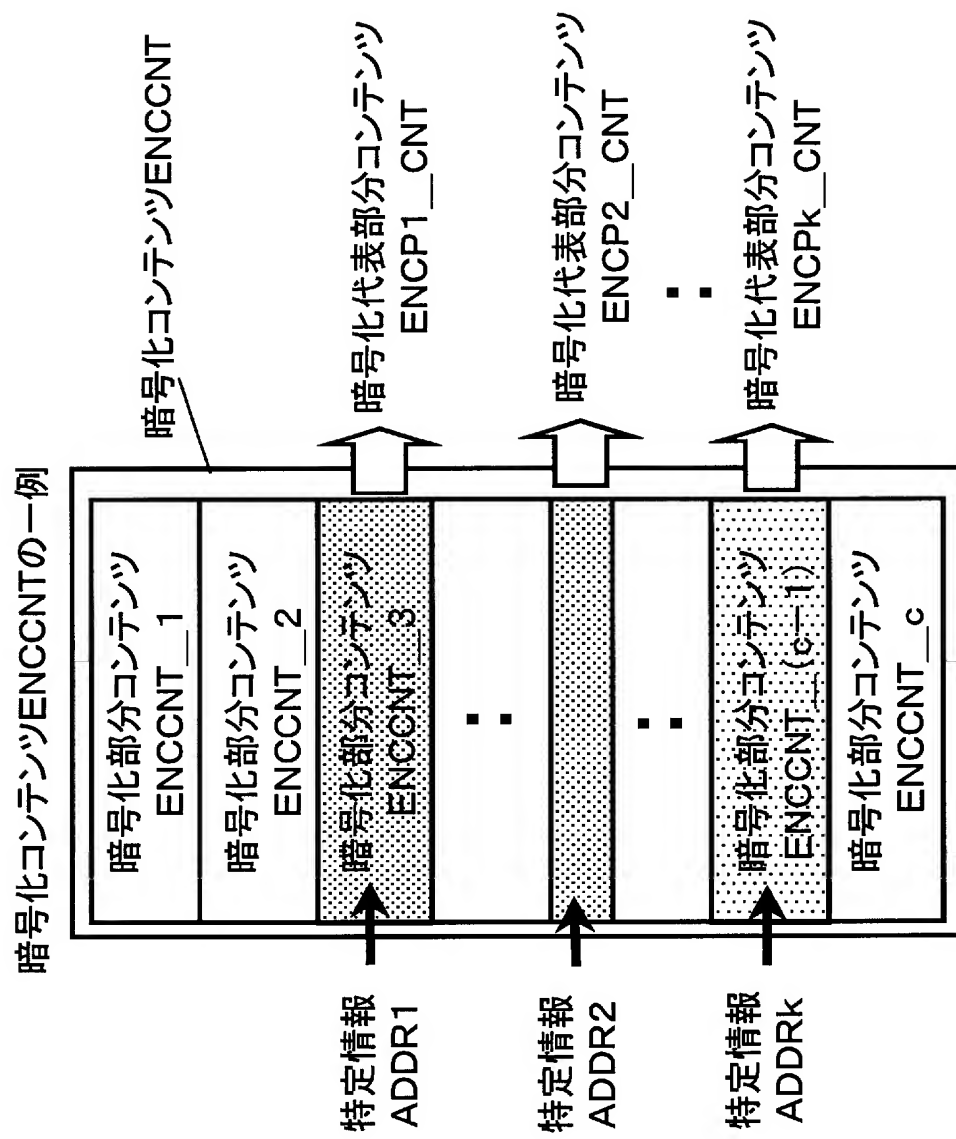


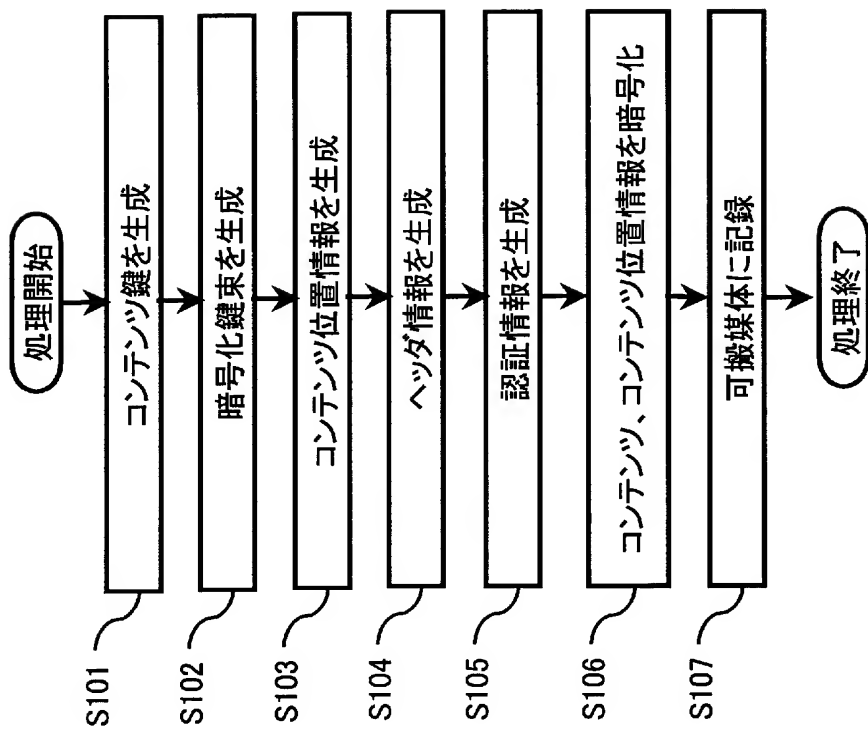
コンテンツ位置情報 POSの一例

特定情報識別子 ADDRID1	特定情報 ADDR1
特定情報識別子 ADDRID2	特定情報 ADDR2
・ ・ ・	・ ・ ・
特定情報識別子 ADDRIDk	特定情報 ADDRk

ヘッダ情報 HEADの一例

特定情報識別子 ADDRID1	ハッシュ値 HASH1
特定情報識別子 ADDRID2	ハッシュ値 HASH2
・ ・ ・	・ ・ ・
特定情報識別子 ADDRIDk	ハッシュ値 HASHk

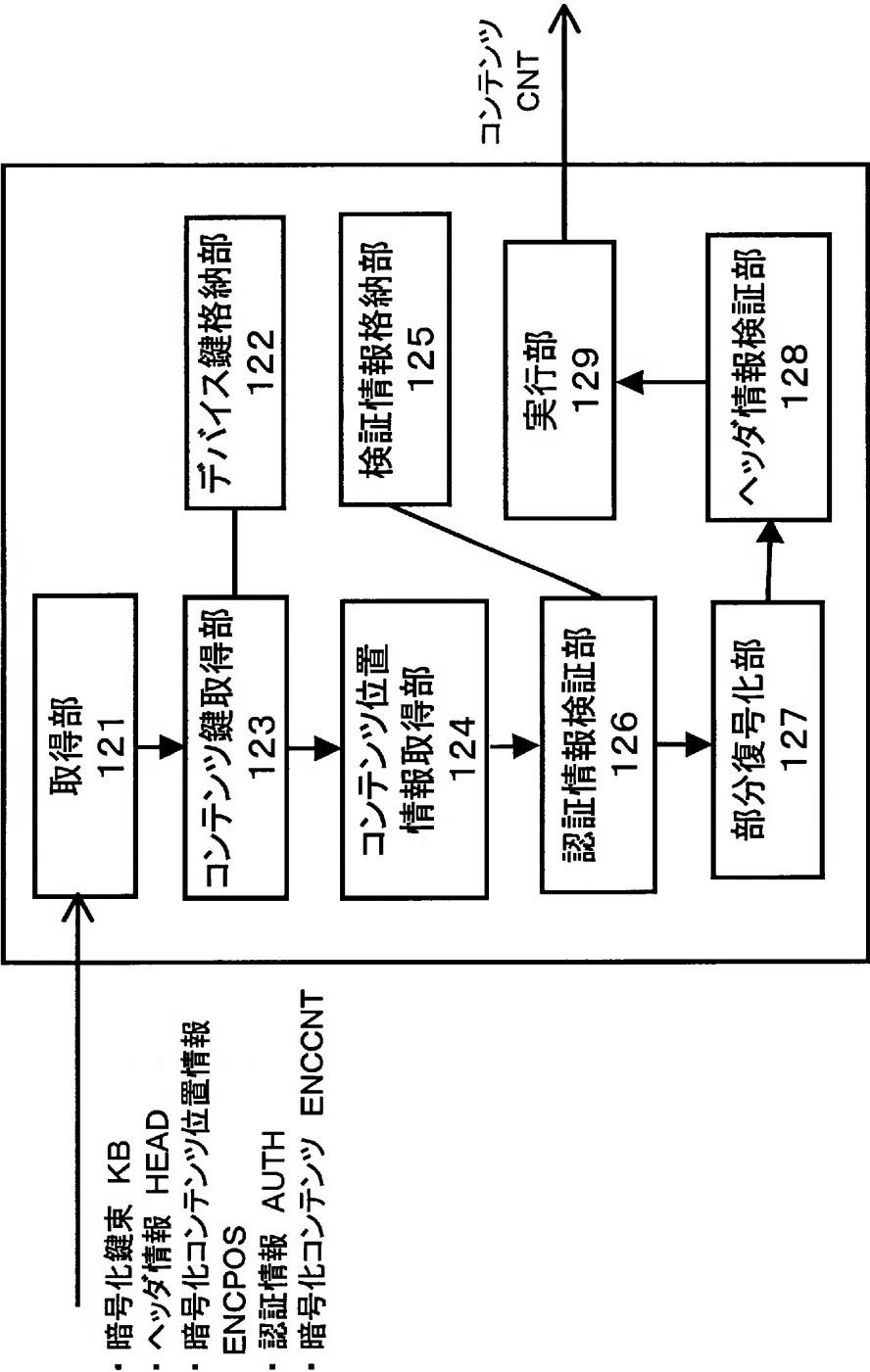


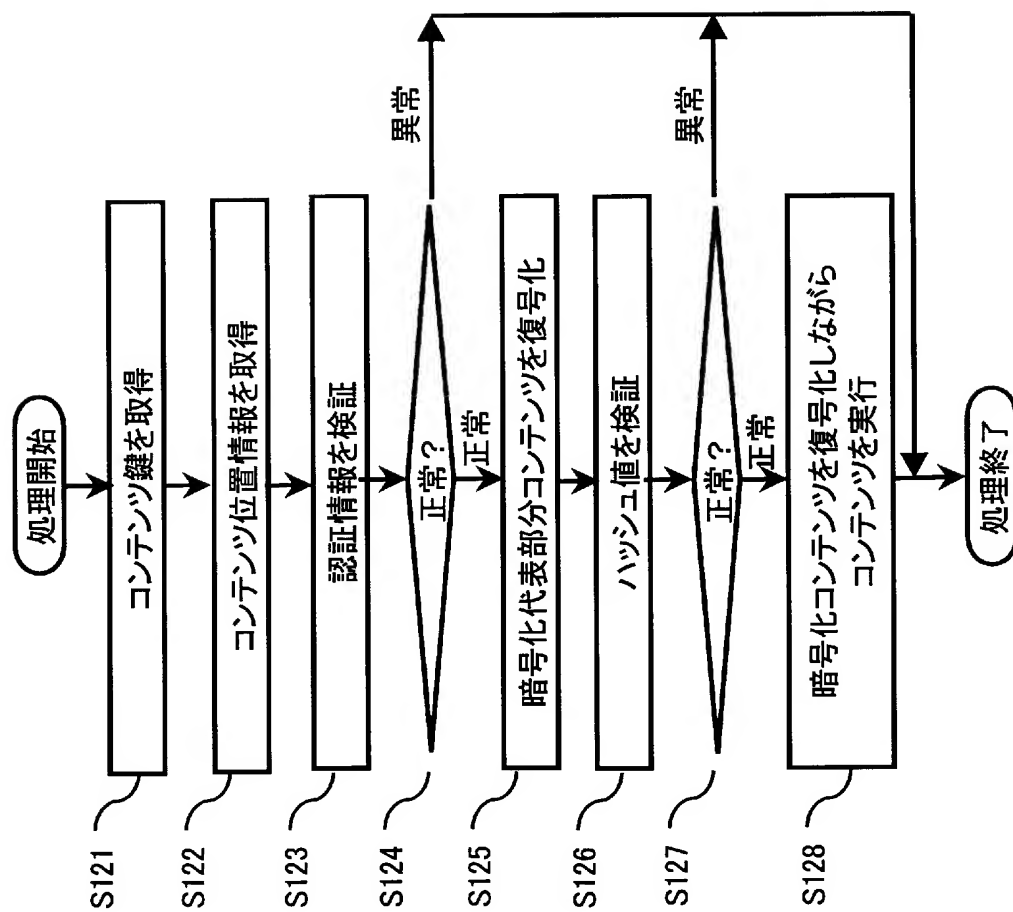


可搬媒体 11 に記録されるデータの一例

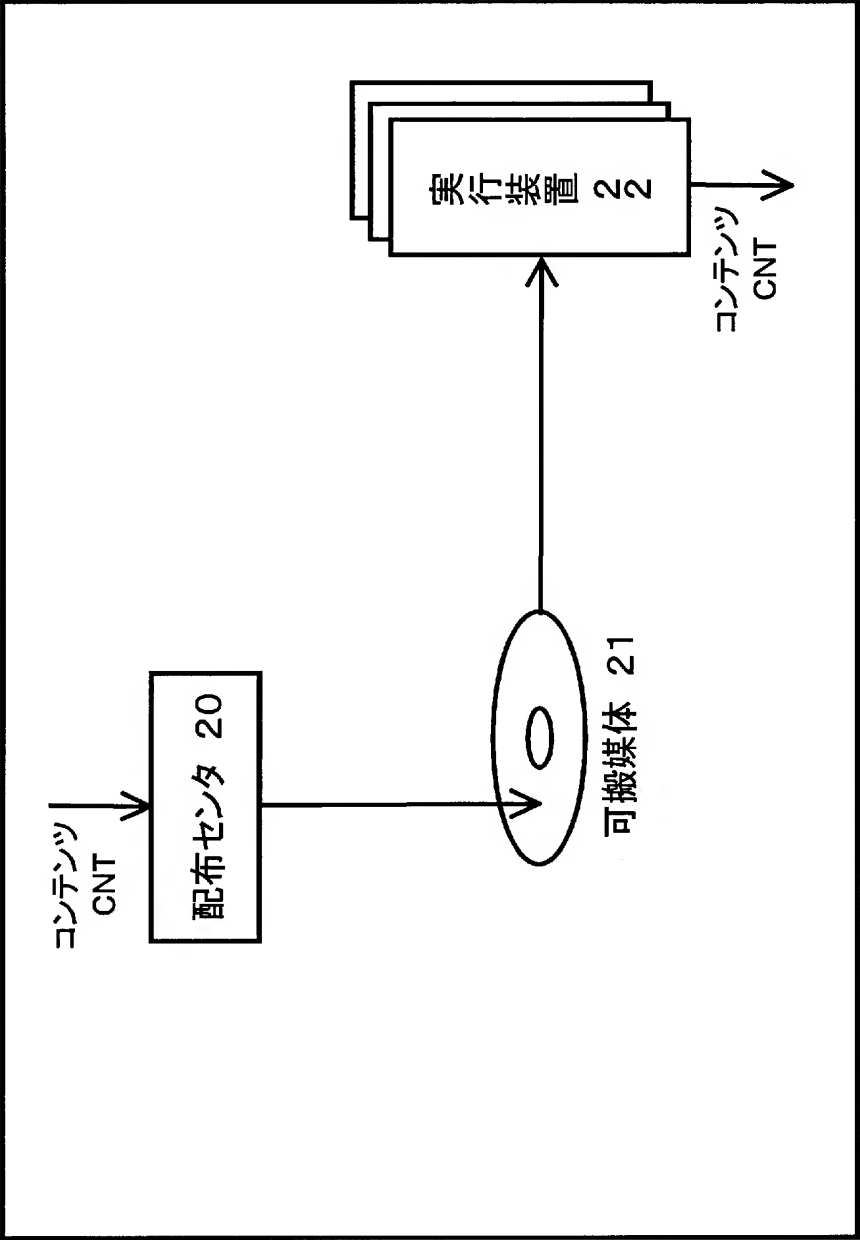
暗号化鍵束 KB
ヘッダ情報 HEAD
暗号化コンテンツ位置情報 ENCPOS
認証情報 AUTH
暗号化コンテンツ ENCCNT

実行装置 12 の一例

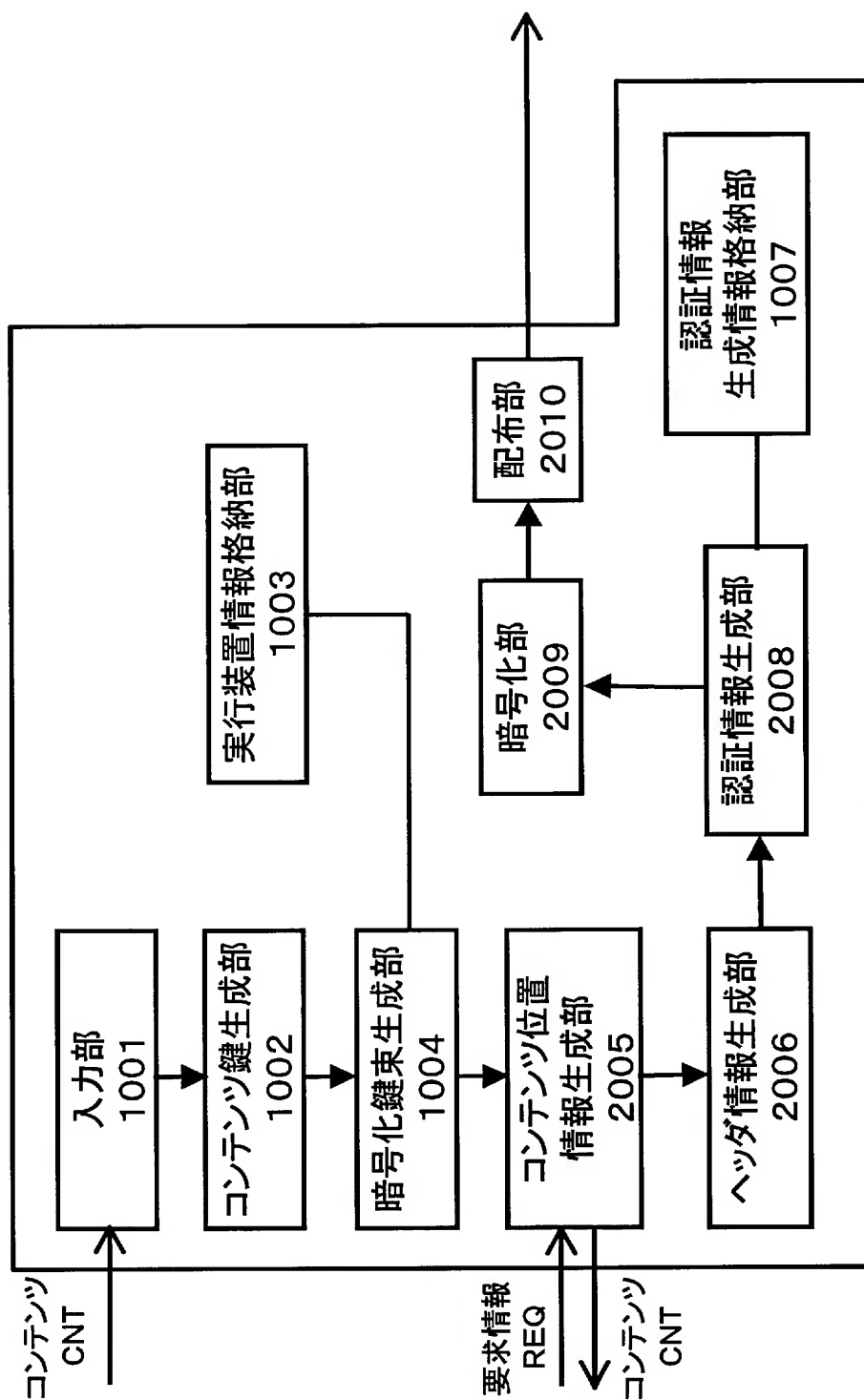


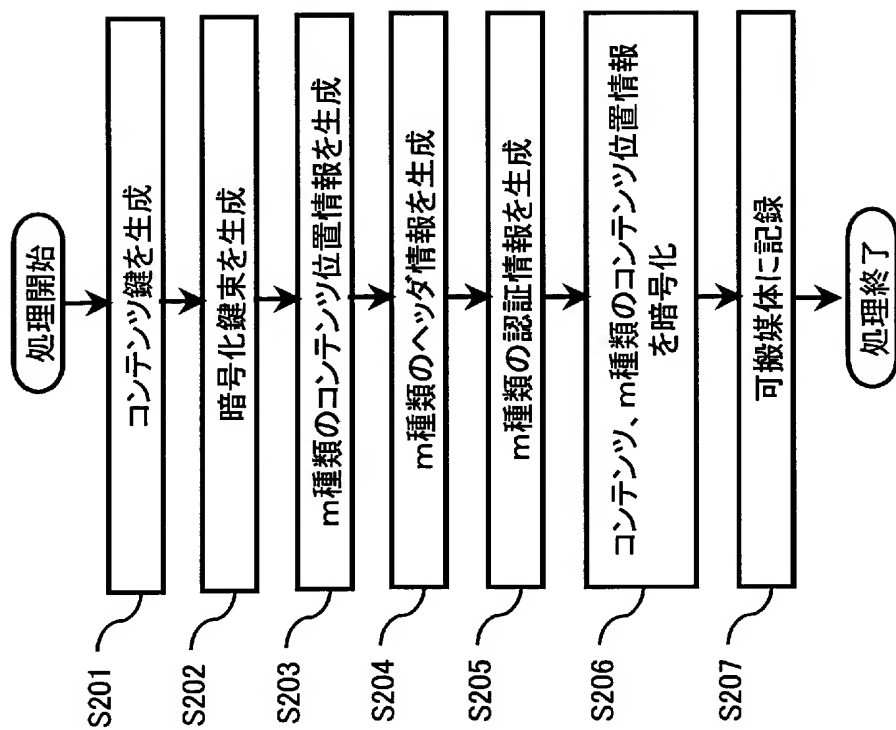


不正コンテンツ検知システム2



配布センタ 20 の一例

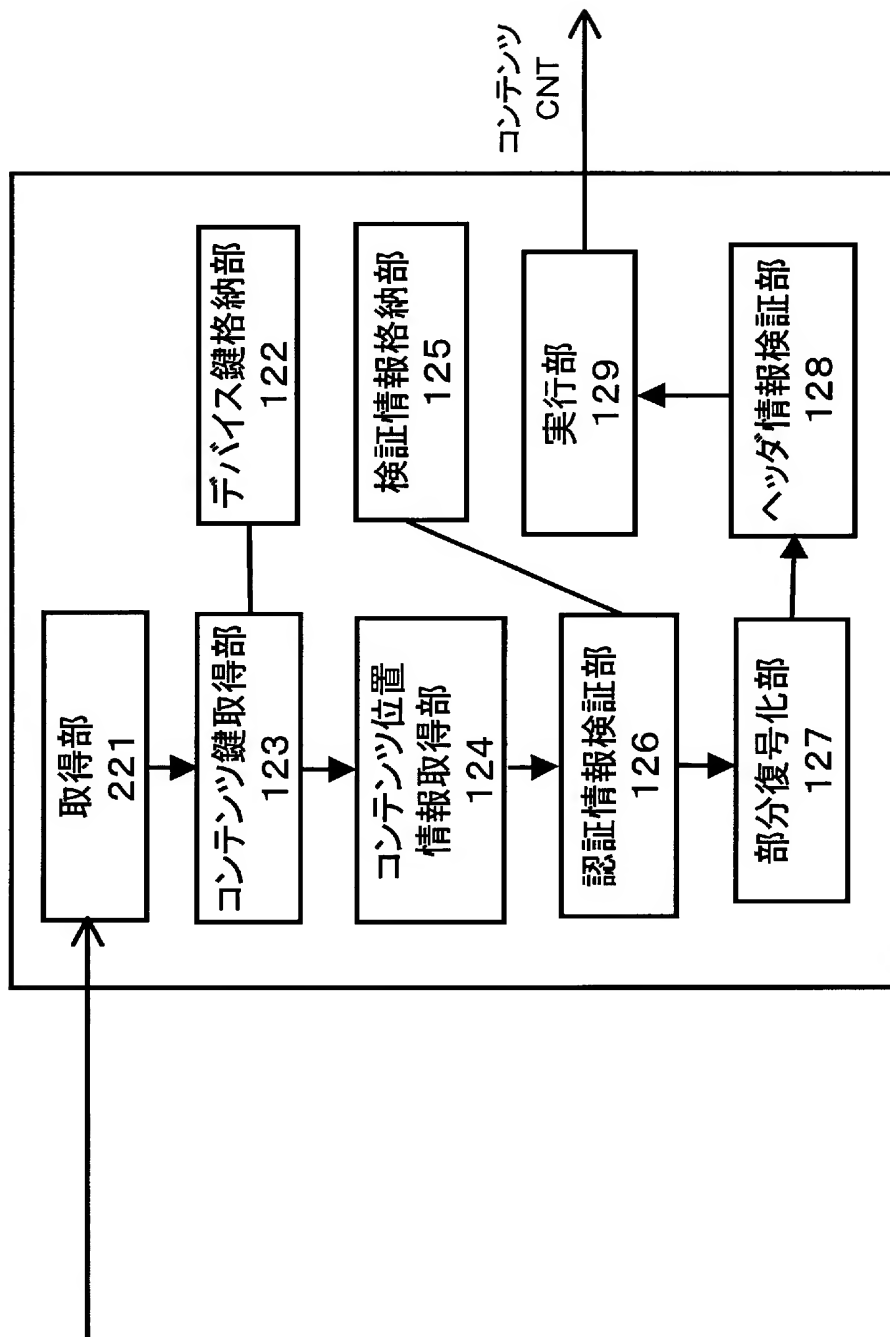


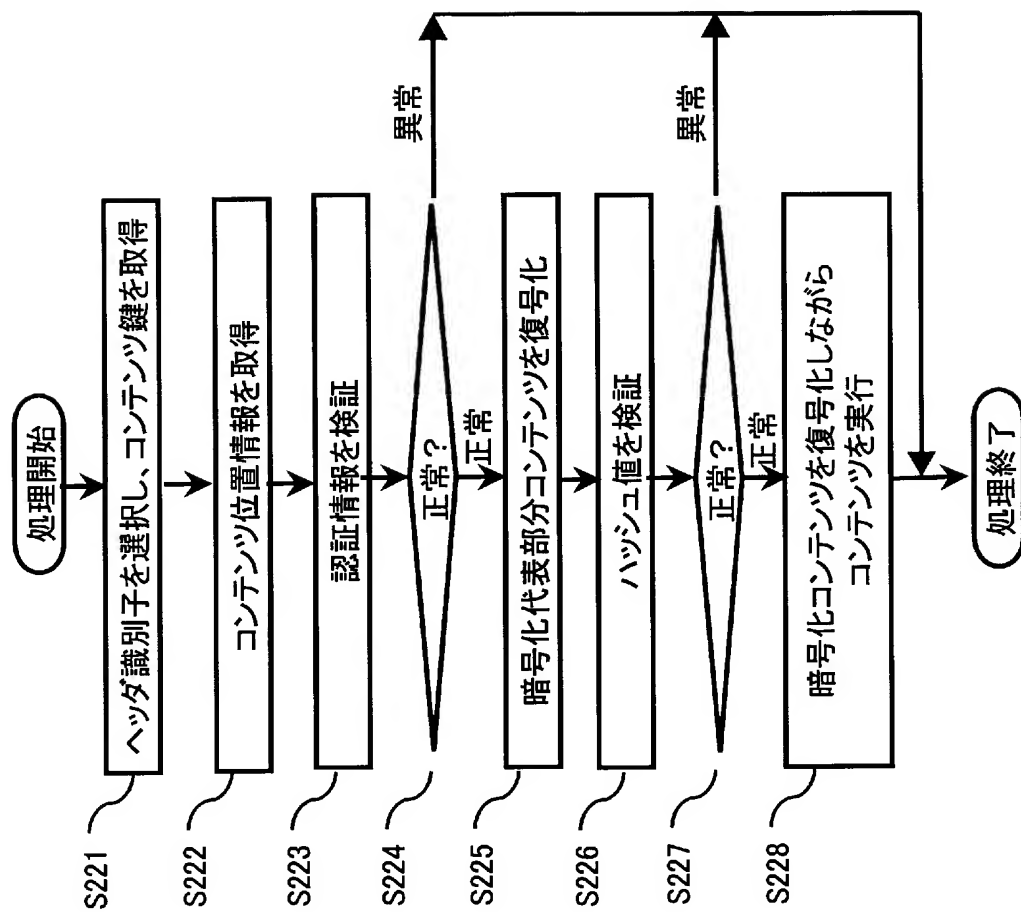


可搬媒体21に記録されるデータの一例

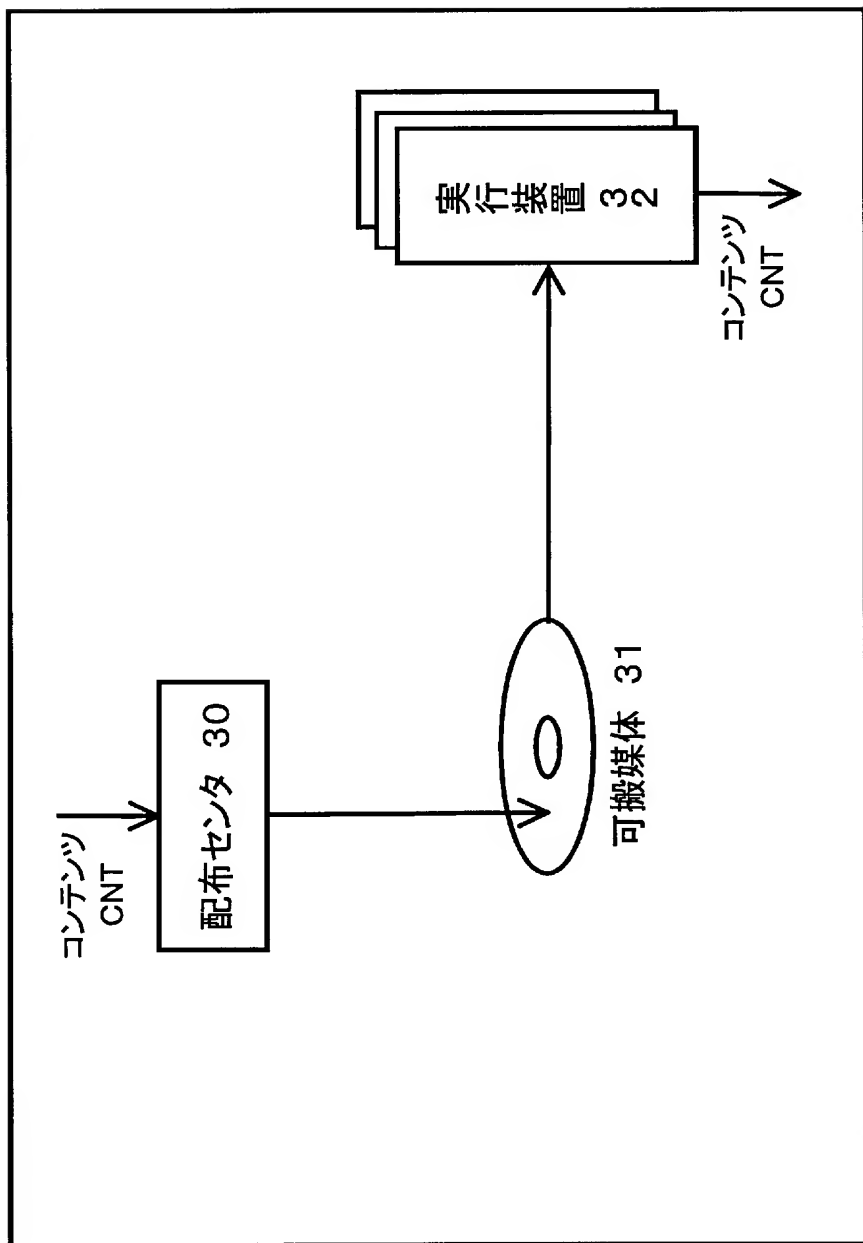
暗号化鍵束 KB				
ヘッダ識別子 HEADID1	ヘッダ識別子 HEADID2	...	ヘッダ識別子 HEADIDm	
ヘッダ情報 HEAD1	ヘッダ情報 HEAD2	...	ヘッダ情報 HEADm	
暗号化コンテンツ 位置情報 ENCPOS1	暗号化コンテンツ 位置情報 ENCPOS2	...	暗号化コンテンツ 位置情報 ENCPOSm	
認証情報 AUTH1	認証情報 AUTH2	...	認証情報 AUTHm	
暗号化コンテンツ ENCCNT				

実行装置 22 の一例

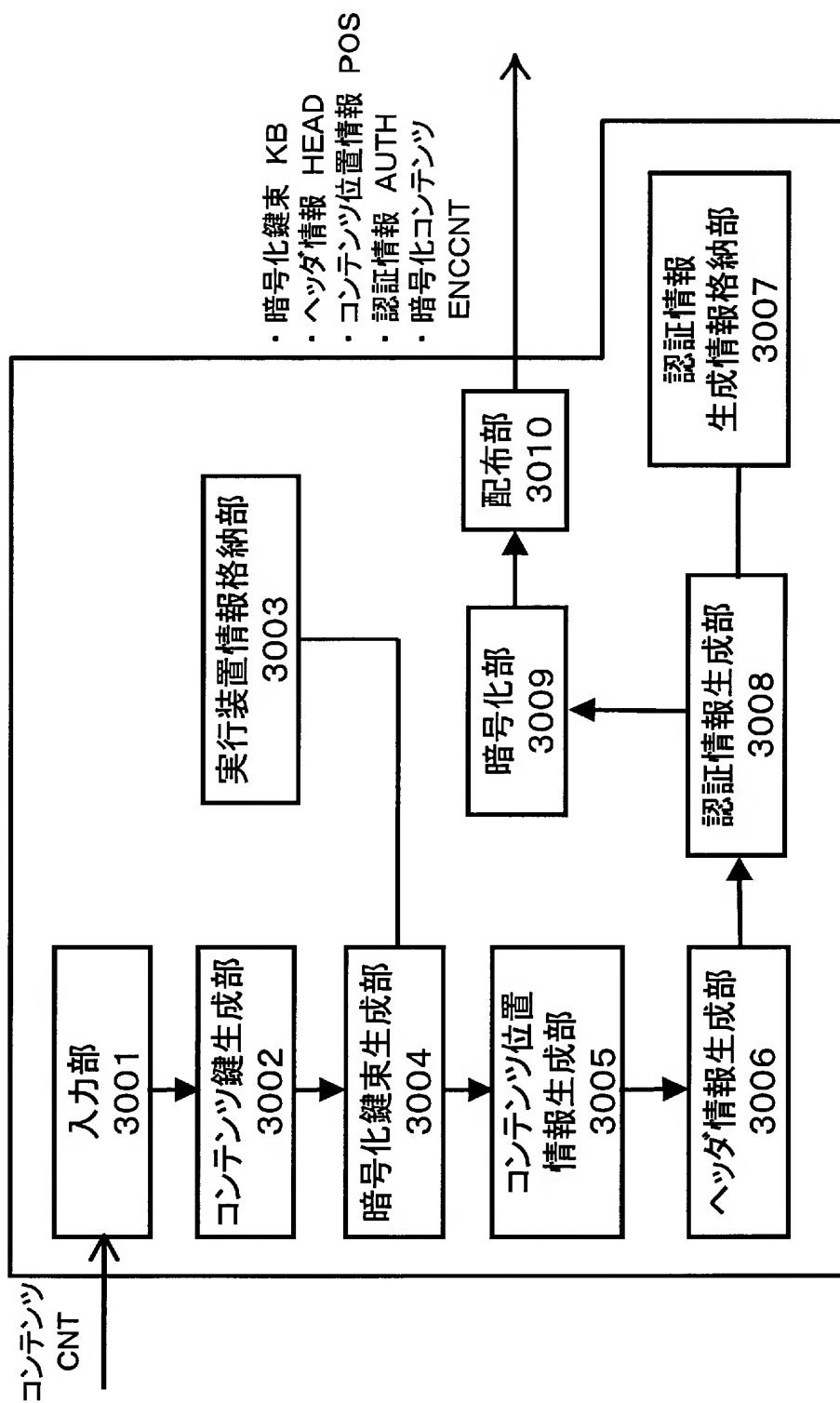




不正コンテンツ検知システム3



配布センタ 30 の一例

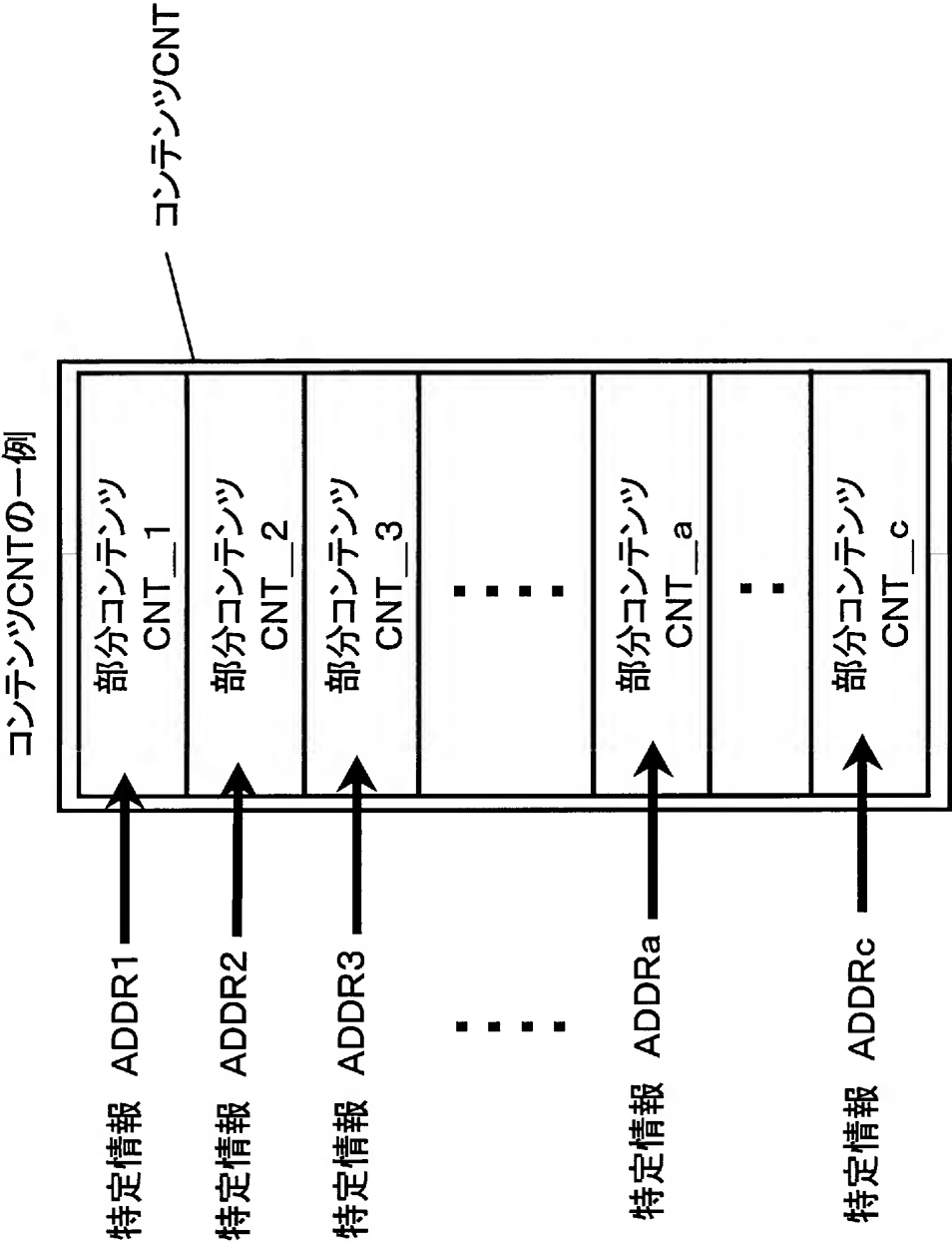


実行装置情報格納部3003の一例

装置識別子 AID1	デバイス鍵 DK1
装置識別子 AID2	デバイス鍵 DK2
装置識別子 AID3	デバイス鍵 DK3
・ ・ ・	・ ・ ・
装置識別子 AIDn	デバイス鍵 DKn

暗号化鍵束 KBの一例



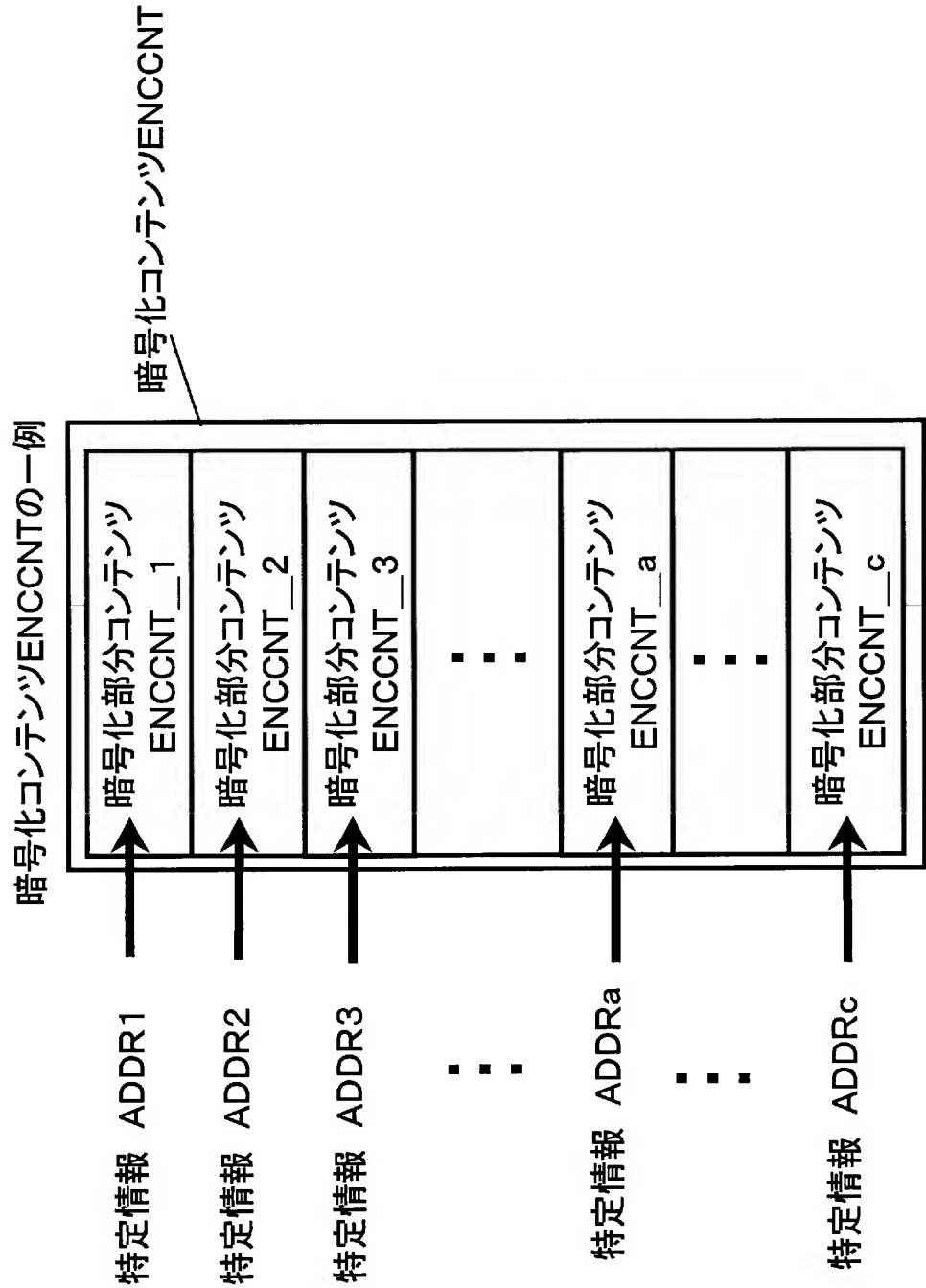


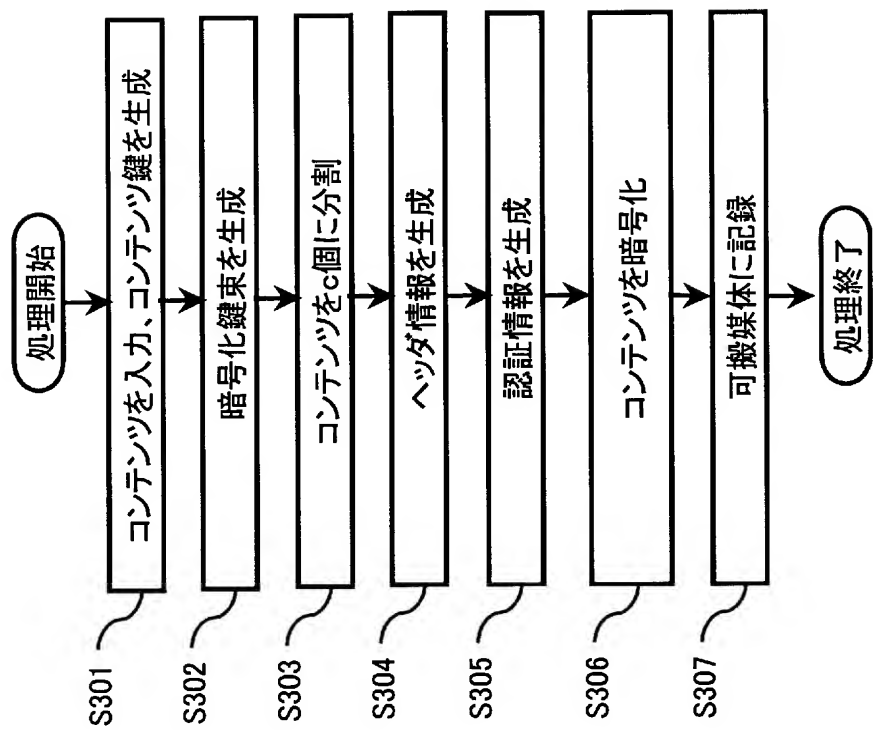
コンテンツ位置情報 POSの一例

特定情報識別子 ADDRID1	特定情報 ADDR1
特定情報識別子 ADDRID2	特定情報 ADDR2
特定情報識別子 ADDRID3	特定情報 ADDR3
▪ ▪ ▪	▪ ▪ ▪
特定情報識別子 ADDRIDa	特定情報 ADDRa
▪ ▪ ▪	▪ ▪ ▪
特定情報識別子 ADDRIDc	特定情報 ADDRc

ヘッダ情報 HEADの一例

特定情報識別子 ADDRID1	ハッシュ値 HASH1
特定情報識別子 ADDRID2	ハッシュ値 HASH2
特定情報識別子 ADDRID3	ハッシュ値 HASH3
▪ ▪ ▪	▪ ▪ ▪
特定情報識別子 ADDRIDa	ハッシュ値 HASHa
▪ ▪ ▪	▪ ▪ ▪
特定情報識別子 ADDRIDc	ハッシュ値 HASHc

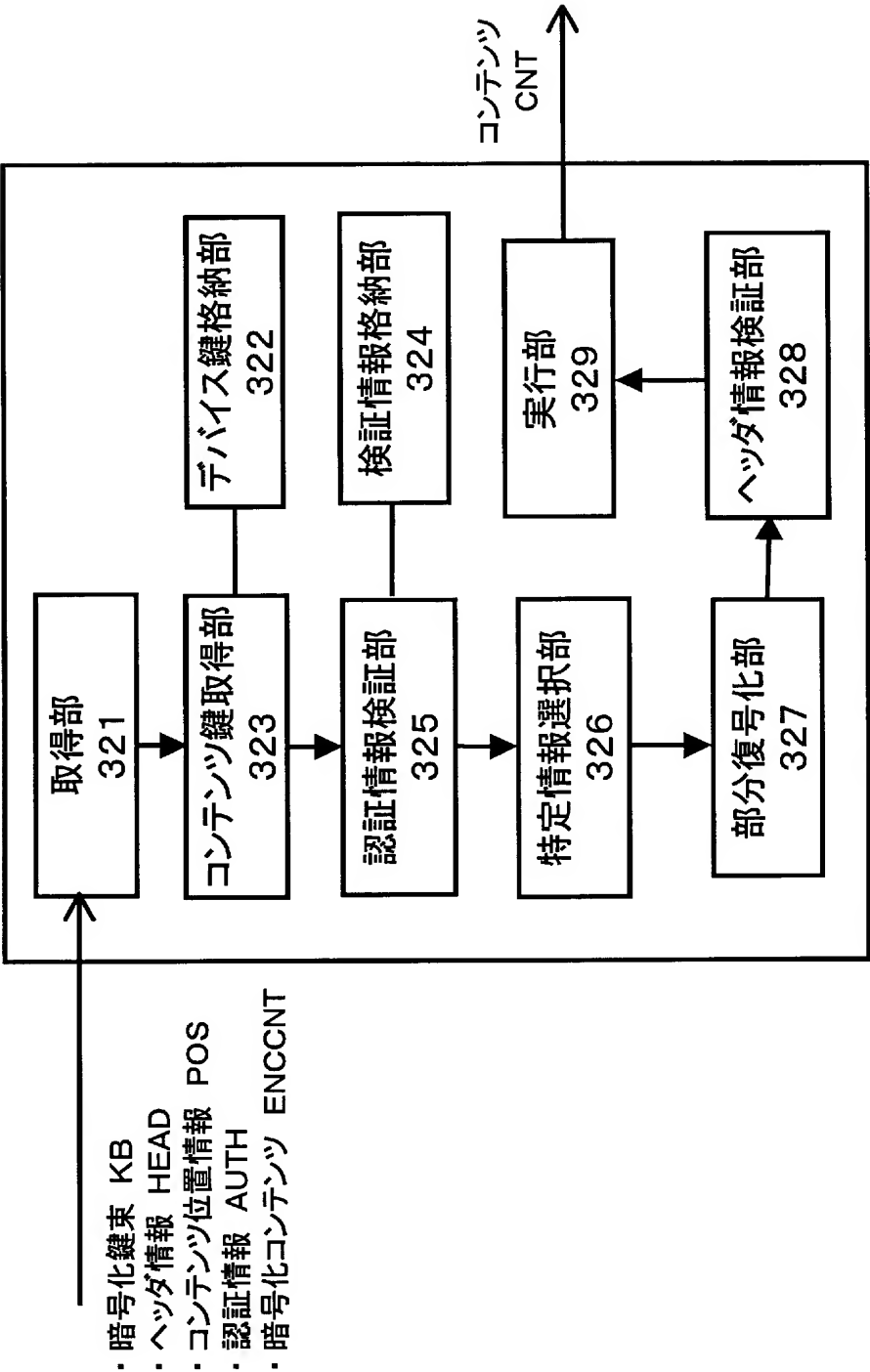




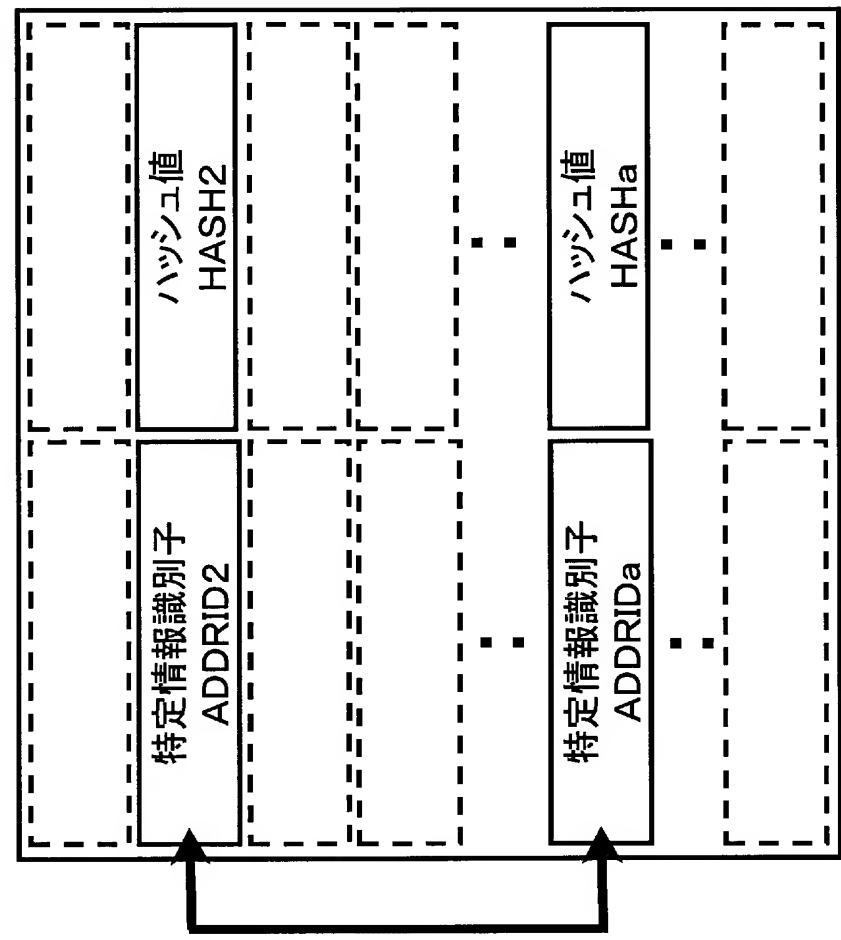
可搬媒体31に記録されるデータの一例

暗号化鍵束 KB	
ヘッダ情報 HEAD	
コンテンツ位置情報 POS	
認証情報 AUTH	
暗号化コンテンツ ENCNT	

実行装置 32 の一例

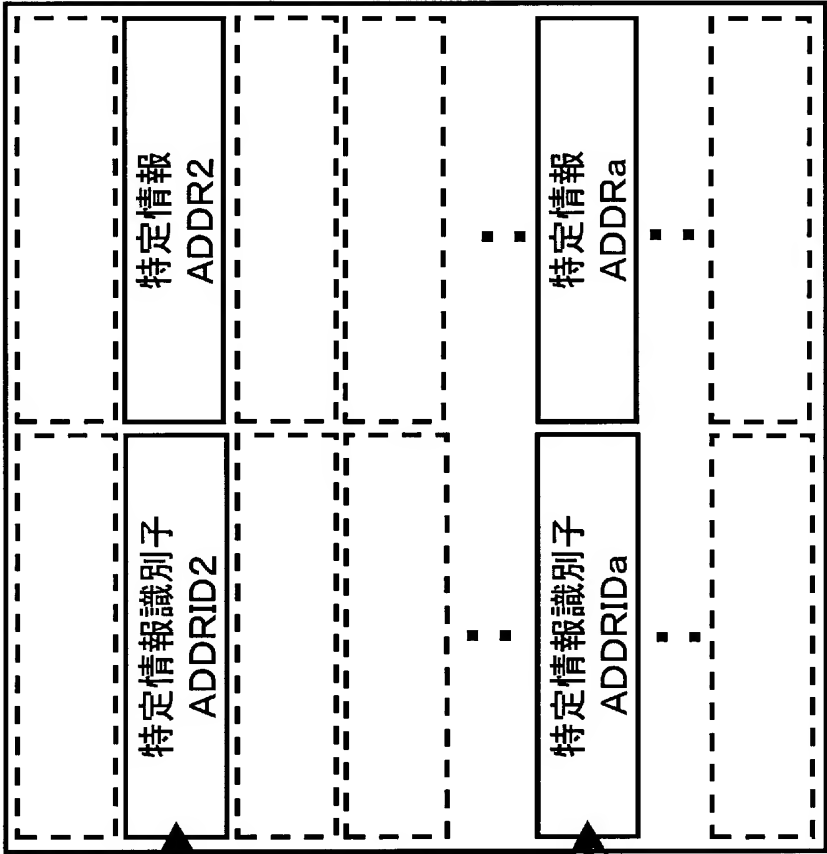


被選択ヘッダ情報 SELHEADの一例



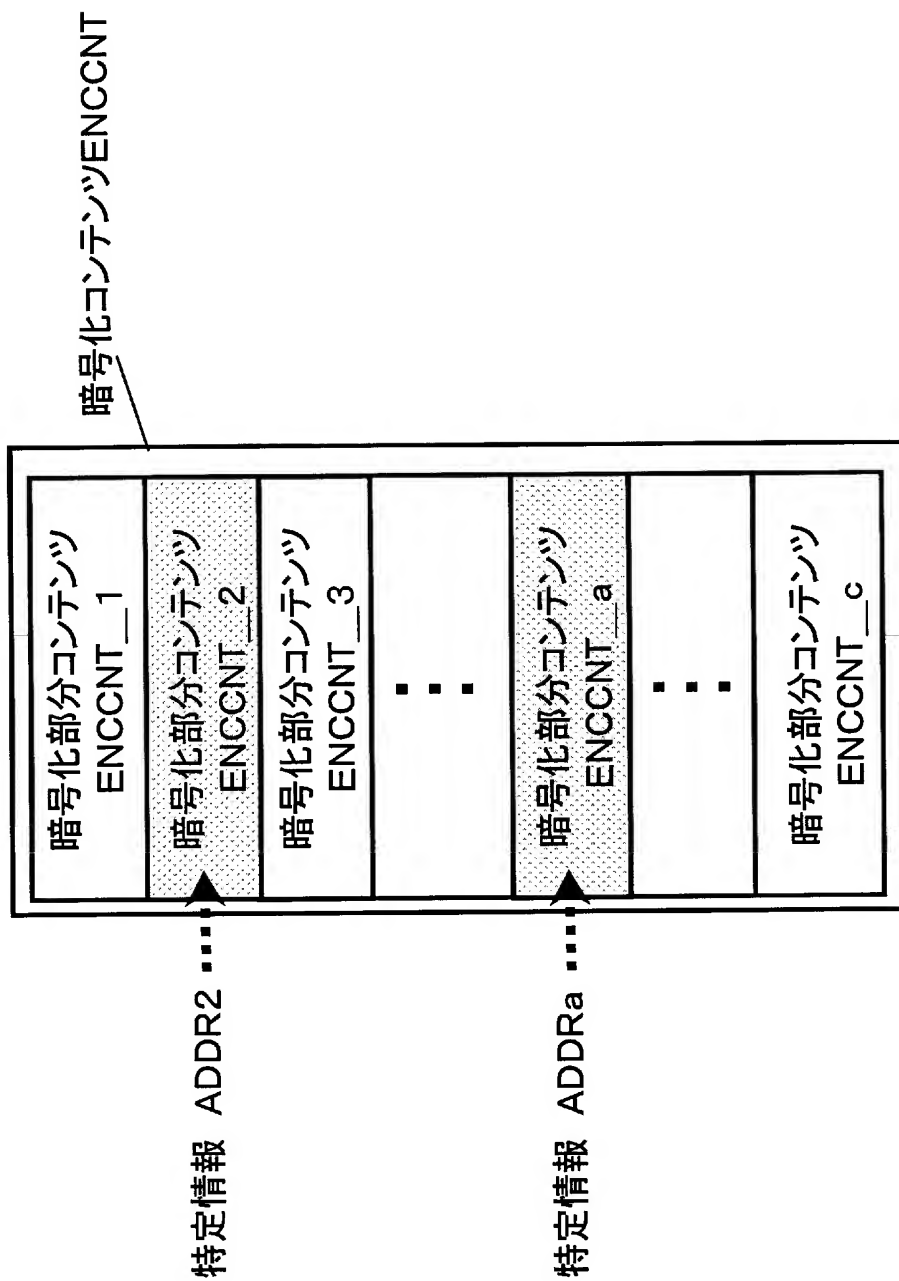
ヘッダ情報HEADから
b組の特定情報識別子と
ハッシュ値を選択

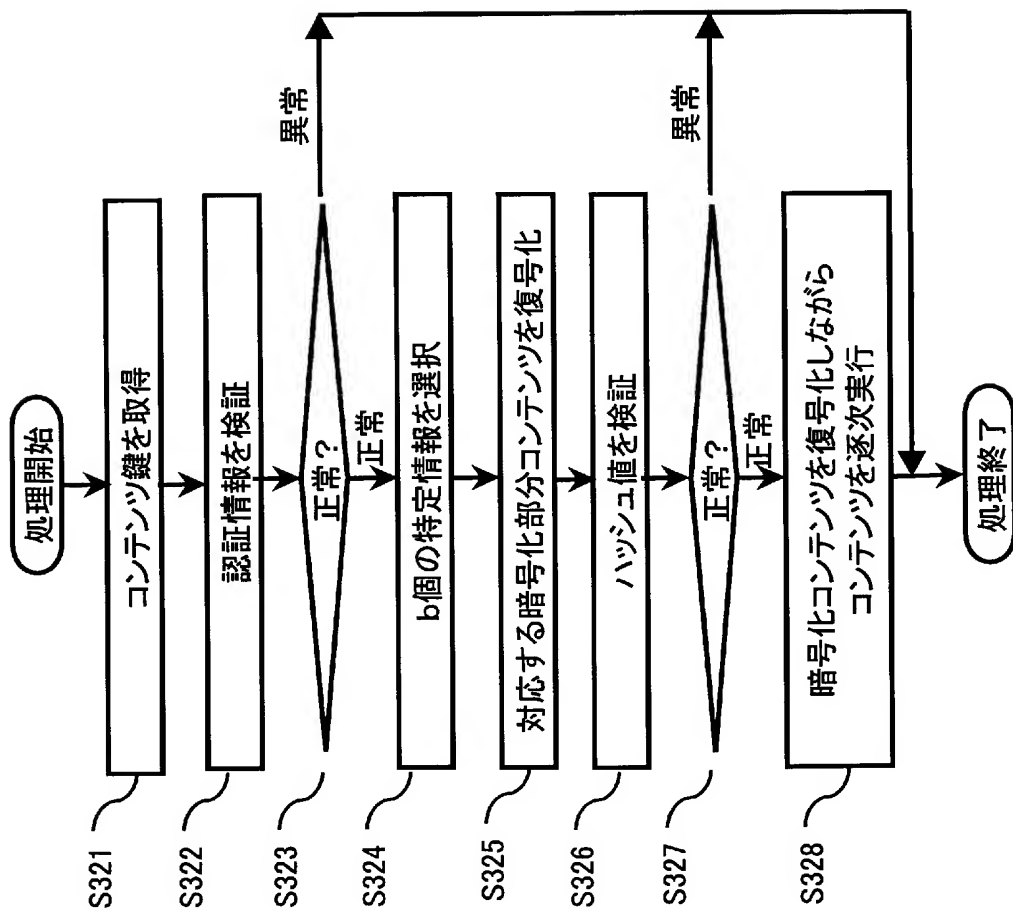
被選択コンテンツ位置情報 SELPOSの一例



コンテンツ位置情報POSから
b組の特定情報識別子と
特定情報を選択

暗号化コンテンツENCNTの一例





可搬媒体に記録されるデータの別の一例

暗号化鍵束 KB
ヘッダ情報 HEAD
コンテンツ位置情報 POS
認証情報 AUTH
暗号化コンテンツ ENCCNT

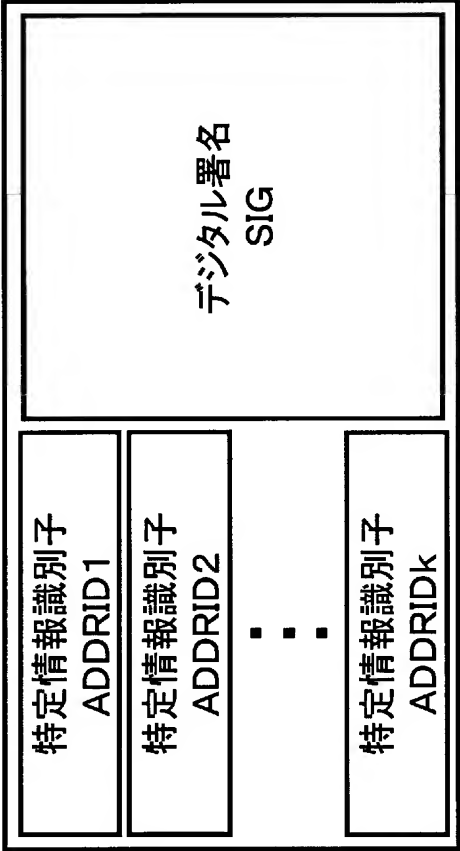
可搬媒体11に記録されるデータの別の一例

暗号化鍵束 KB	
コンテンツ認証情報 CNTAUTH	
暗号化コンテンツ ENCNT	

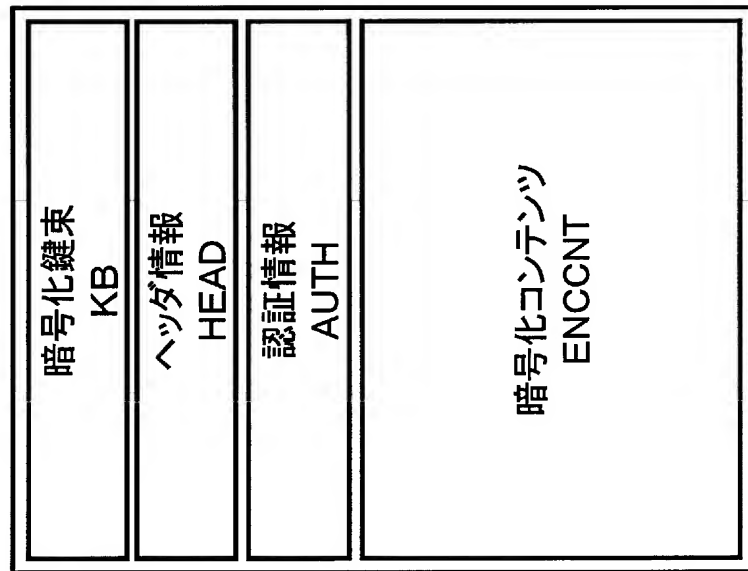
コンテンツ認証情報 CNTAUTHの一例

特定情報識別子 ADDRID1	デジタル署名 S1
特定情報識別子 ADDRID2	デジタル署名 S2
・ ・ ・	・ ・ ・
特定情報識別子 ADDRIDk	デジタル署名 Sk

コンテンツ認証情報 CNTAUTHの別の一例



可搬媒体111に記録されるデータの別の別の一例



可搬媒体11に記録されるデータの別の例

暗号化鍵束 KB
ヘッダ情報 HEAD
コンテンツ位置情報識別子 CNTAIDi
認証情報 AUTH
暗号化コンテンツ ENCCNT

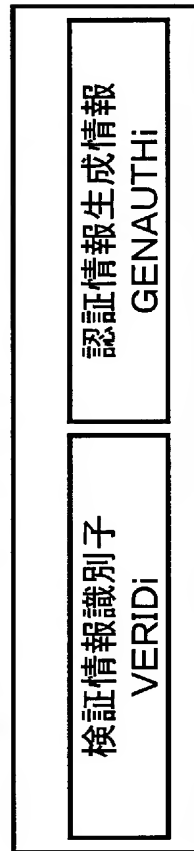
認証情報AUTHを作成する
ヘッダ情報HEADの別の一例

特定情報識別子 ADDRID1	ハッシュ値 HASH1
特定情報識別子 ADDRID2	ハッシュ値 HASH2
・ ・ ・	・ ・ ・
特定情報識別子 ADDRIDk	ハッシュ値 HASHk
コンテンツ鍵 CK	

ヘッダ情報HEADの別の一例

特定情報識別子 ADDRID1	ハッシュ値 HASH1
特定情報識別子 ADDRID2	ハッシュ値 HASH2
・ ・ ・	・ ・ ・
特定情報識別子 ADDRIDk	ハッシュ値 HASHk
コンテンツサイズ CNTSIZE	

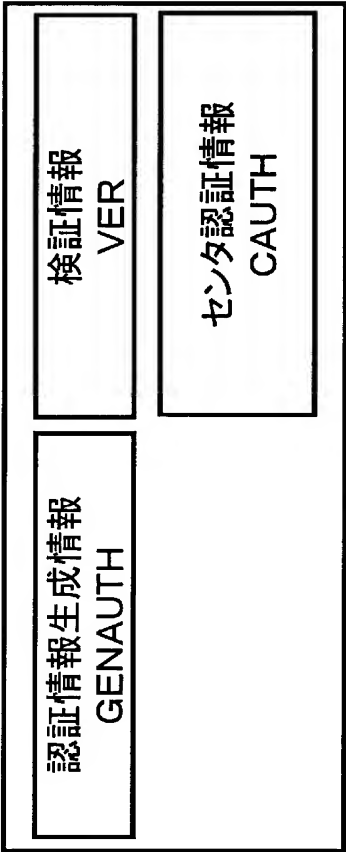
認証情報生成情報格納部1007の別の一例



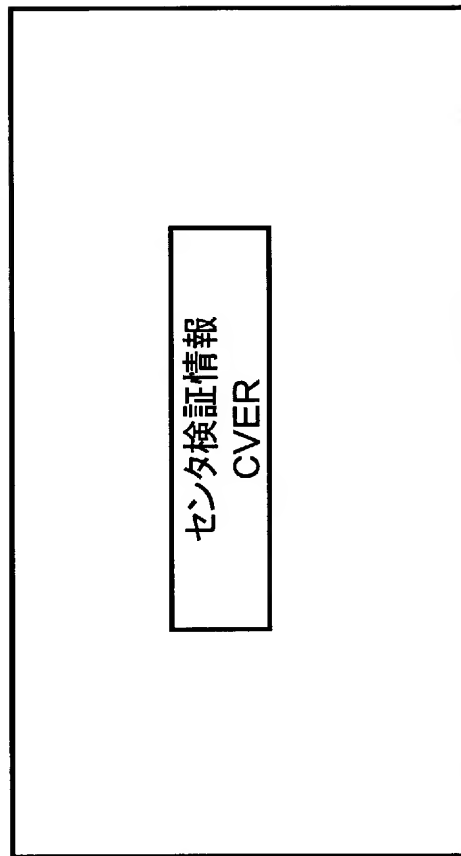
検証情報格納部125の別の例

検証情報識別子 VERID1	検証情報 VER1
検証情報識別子 VERID2	検証情報 VER2
・ ・ ・	・ ・ ・
検証情報識別子 VERIDw	検証情報 VERw

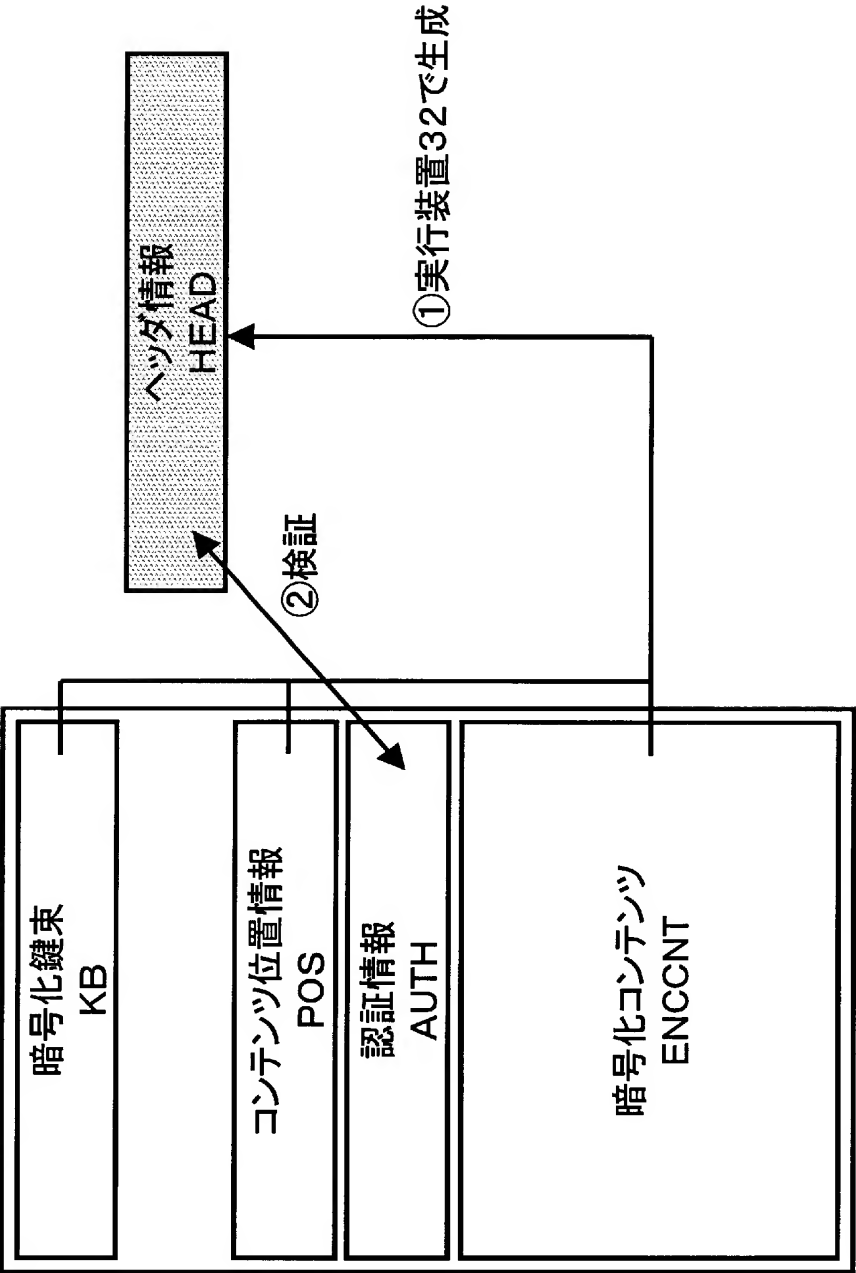
認証情報生成情報格納部1007の別の一例



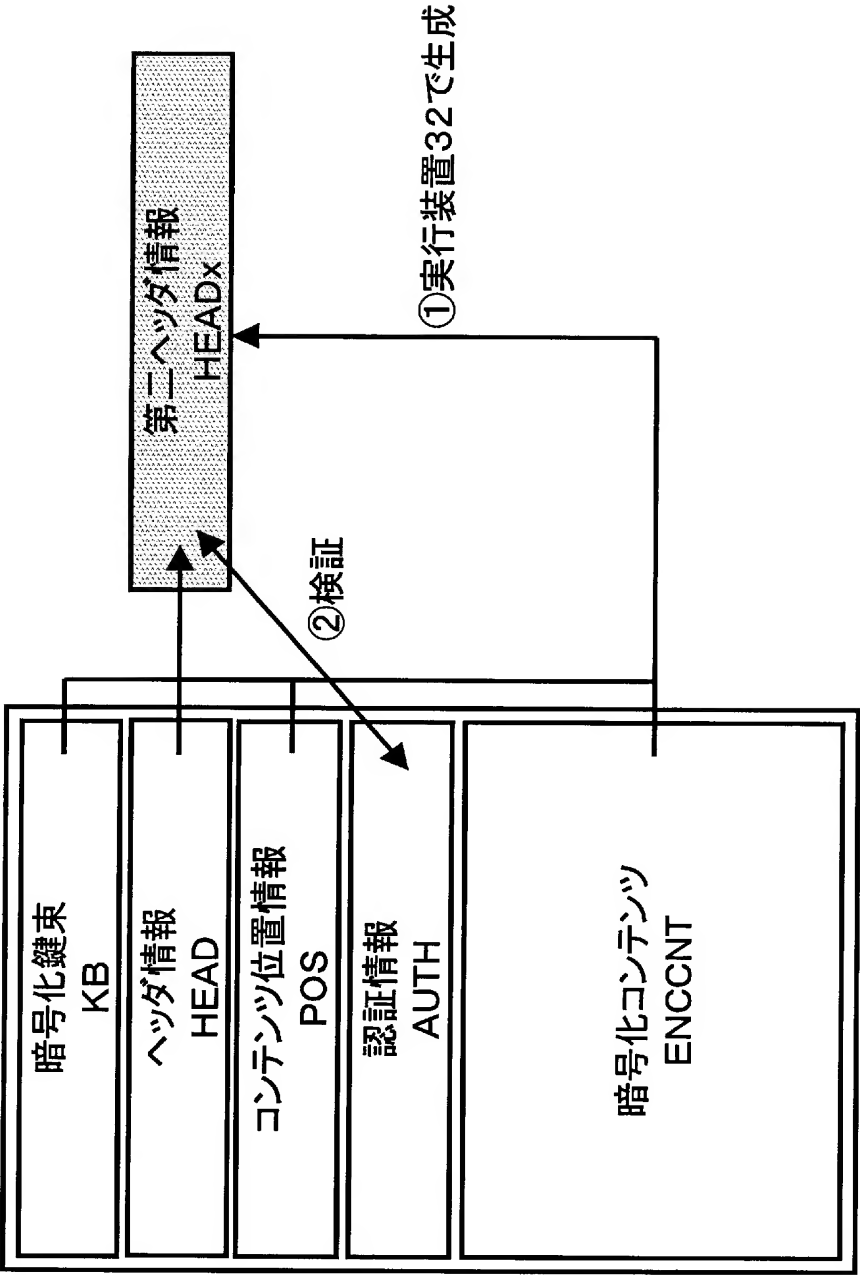
検証情報格納部125の別の例



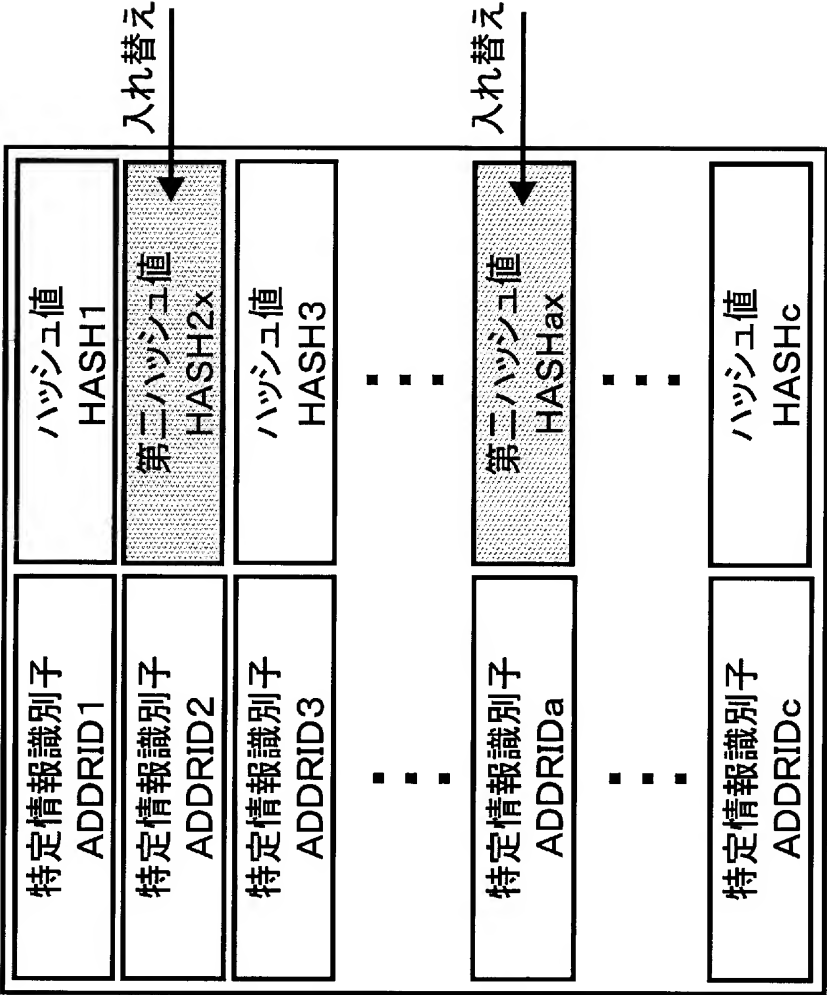
可搬媒体31に記録されるデータ(別の一例)



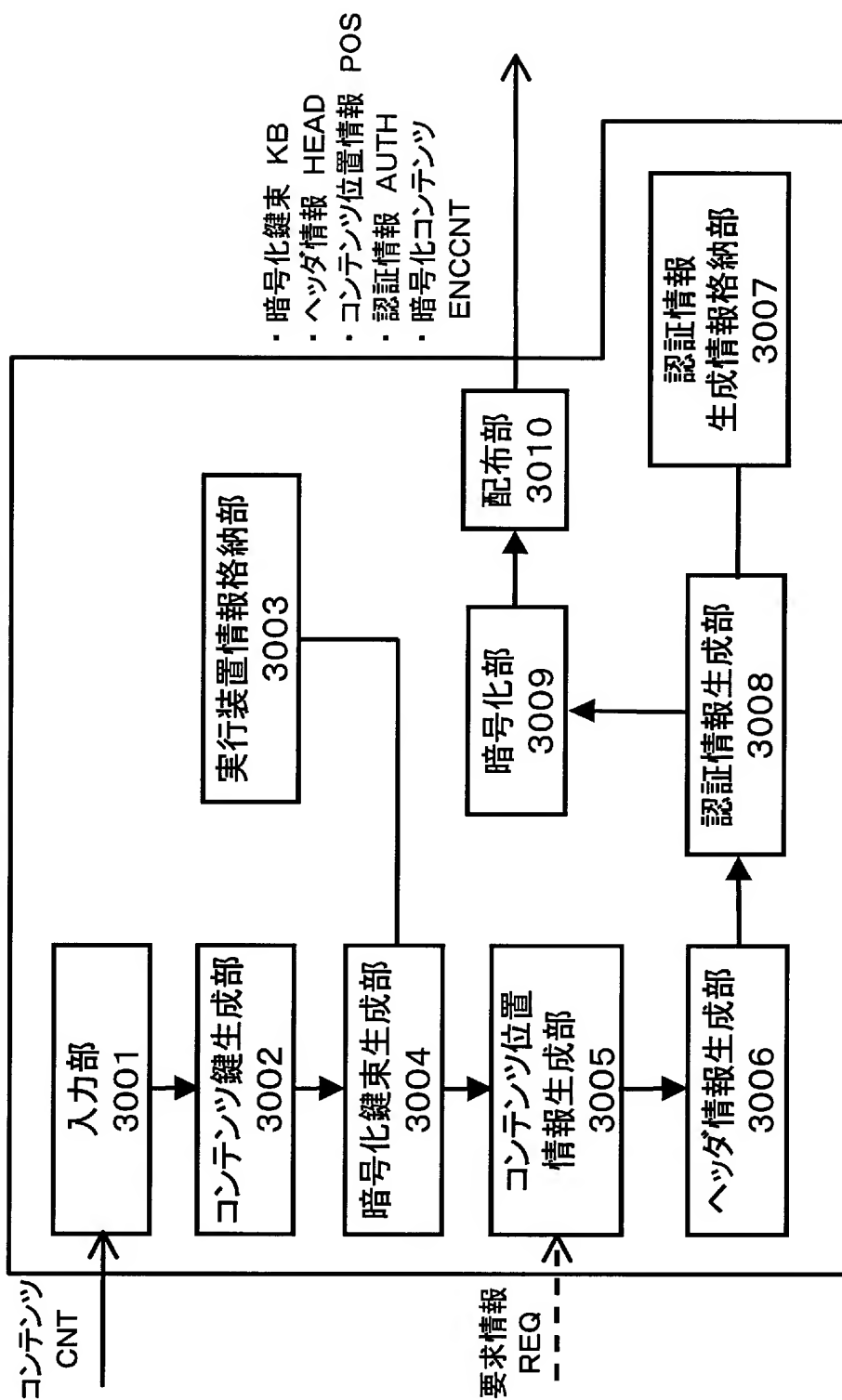
可搬媒体31に記録されるデータ(別の一例)



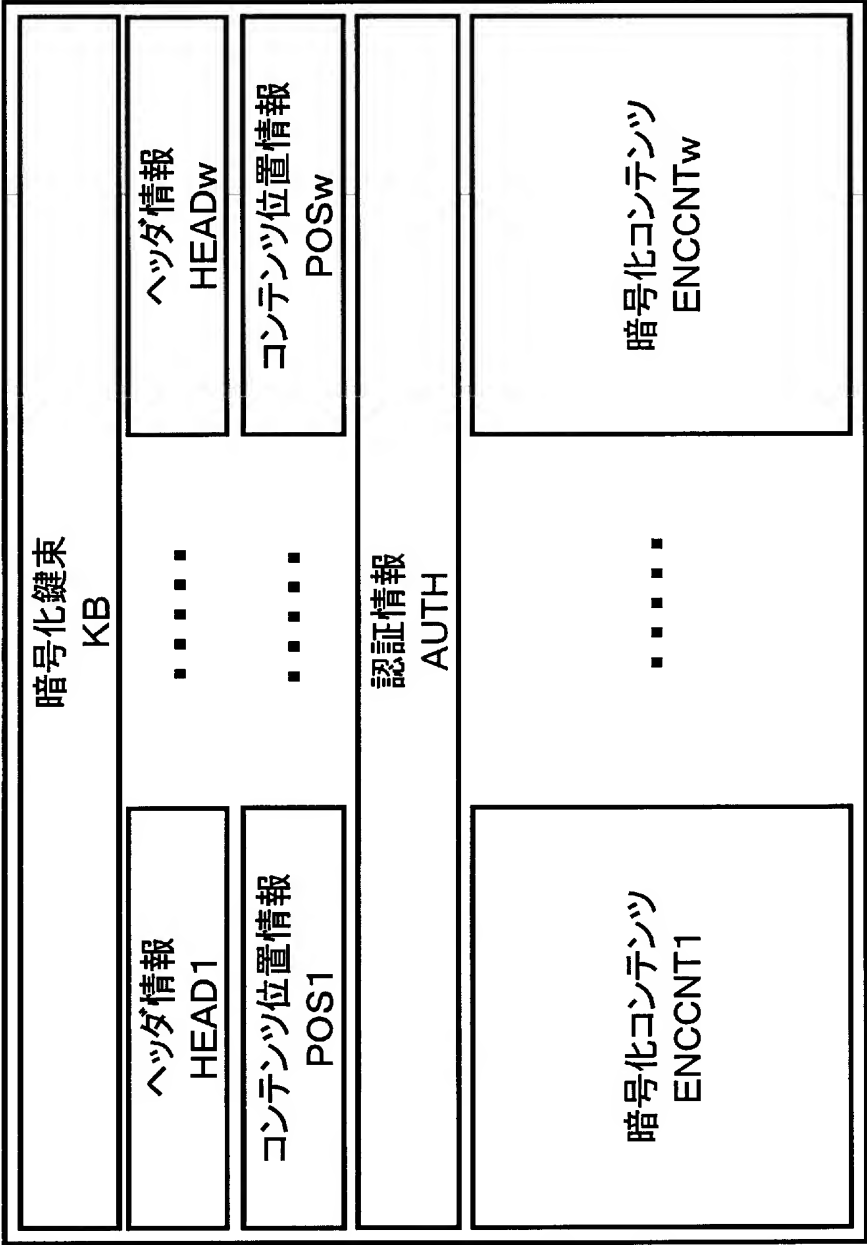
第二ヘッダ情報 HEADxの一例



配布センタ 30 の一例



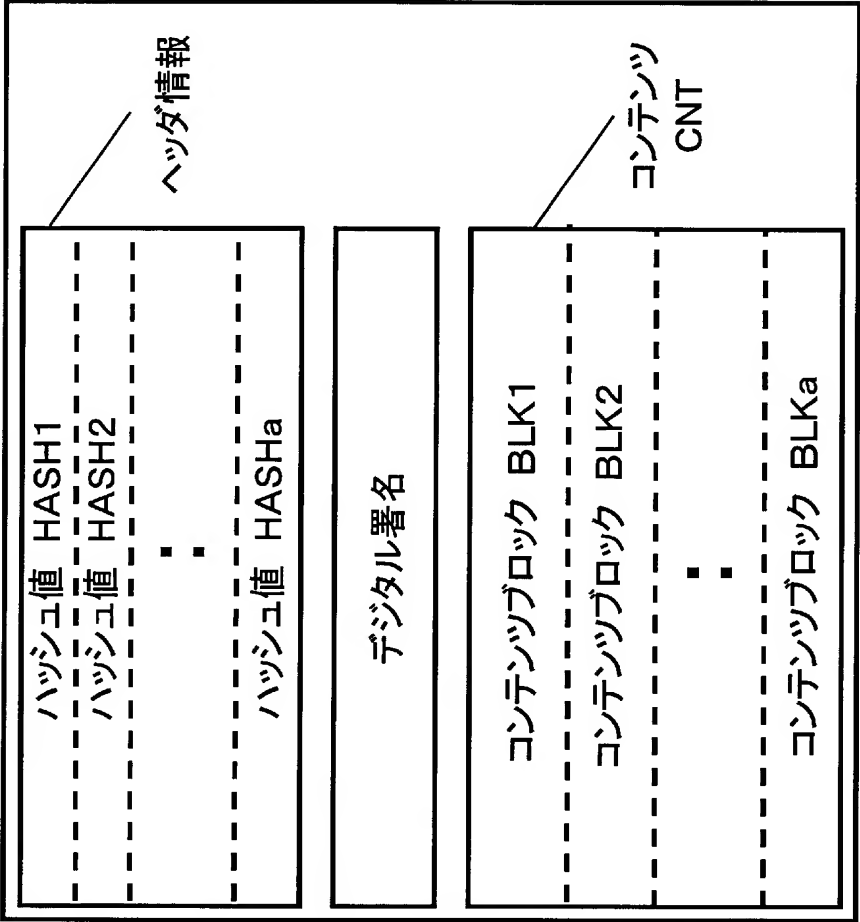
可搬媒体31に記録されるデータの別の一例



可搬媒体31に記録されるデータの別の一例

暗号化鍵束 KB
ヘッダ情報 HEAD
暗号化コンテンツ位置情報 ENCPOS
認証情報 AUTH
暗号化コンテンツ ENCCNT

従来技術の可搬媒体に記録されるデータ



【書類名】 要約書

【要約】

【課題】 実行装置において不正コンテンツかどうか検知する処理において、コンテンツ実行中の処理負荷が大きかった。

【解決手段】 まずコンテンツC N Tを構成するc個の部分コンテンツC N T—1、・ ・ ・、C N T—cの中から、一つの部分コンテンツを選択し、それを代表部分コンテンツP 1—C N Tとする。そして、その代表部分コンテンツP 1—C N Tを指し示す特定情報をA D D R 1とする。そして、続けて、k—1個の代表部分コンテンツP 2—C N T、・ ・ ・、P k—C N Tを選択し、その代表部分コンテンツに対応する特定情報をA D D R 2、・ ・ ・、A D D R kとする。

【選択図】 図6

出願人履歴

0 0 0 0 0 5 8 2 1

19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社